

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Akio HIGASHI et al. :  
Serial No. NEW : **Attn: APPLICATION BRANCH**  
Filed February 26, 2004 : Attorney Docket No. 2004\_0300A  
CONTENT HISTORY LOG COLLECTING SYSTEM

**CLAIM OF PRIORITY UNDER 35 USC 119**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2003-052761, filed February 28, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Akio HIGASHI et al.

By 

Michael S. Huppert  
Registration No. 40,268  
Attorney for Applicants

MSH/kjf  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
February 26, 2004

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 2月28日  
Date of Application:

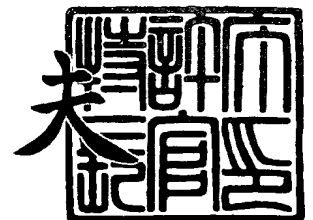
出願番号 特願2003-052761  
Application Number:  
[ST. 10/C]: [JP 2003-052761]

出願人 松下電器産業株式会社  
Applicant(s):

2003年11月11日

特許庁長官  
Commissioner,  
Japan Patent Office

今井 康夫



出証番号 出証特2003-3093091

【書類名】 特許願

【整理番号】 2032750015

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 東 吾紀男

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 三浦 康史

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山本 雅哉

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 村上 弘規

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 徳田 克己

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ利用実績収集システム

【特許請求の範囲】

【請求項 1】 端末装置にコンテンツを配信するコンテンツ配信サーバと、前記コンテンツを利用した利用実績を記録し、前記利用実績を利用実績収集サーバに送信する端末装置と、前記端末装置から前記コンテンツの前記利用実績を収集する利用実績収集サーバと、から構成されるコンテンツ利用実績収集システムであって、

前記コンテンツ配信サーバは、

前記コンテンツを送出するコンテンツ送出手段と、

第 1 の時刻情報を生成する第 1 の時刻情報生成手段と、

前記第 1 の時刻情報を、前記コンテンツ送出手段から送出する前記コンテンツに付加する第 1 の時刻情報付加手段と、

前記コンテンツの先頭における前記第 1 の時刻情報を第 2 の時刻情報として記録する第 2 の時刻情報記録手段と、

を備え、

前記端末装置は、

前記コンテンツを利用するコンテンツ利用手段と、

前記コンテンツに付加された少なくとも前記第 1 の時刻情報を、前記コンテンツ利用手段で利用した前記コンテンツの利用実績として記録する第 1 の時刻情報記録手段と、

前記第 1 の時刻情報を前記利用実績収集サーバに送信する利用実績送信手段と

を備え、

前記利用実績収集サーバは、

前記端末装置から少なくとも前記第 1 の時刻情報を取得する第 1 の時刻情報取得手段と、

前記コンテンツ配信サーバから少なくとも前記第 2 の時刻情報を取得する第 2 の時刻情報取得手段と、

前記第 1 の時刻情報と前記第 2 の時刻情報とから、前記コンテンツの利用部分を特定可能な相対時刻情報を算出する利用実績取得手段と、  
を備えることを特徴とするコンテンツ利用実績収集システム。

【請求項 2】 端末装置にコンテンツを配信するコンテンツ配信サーバと、前記コンテンツを利用した利用実績を記録し、前記利用実績を利用実績収集サーバに送信する端末装置と、前記端末装置から前記コンテンツの前記利用実績を収集する利用実績収集サーバと、から構成されるコンテンツ利用実績収集システムであって、

前記コンテンツ配信サーバは、  
前記コンテンツを送出するコンテンツ送出手段と、  
第 1 の時刻情報を生成する第 1 の時刻情報生成手段と、  
前記コンテンツの先頭における前記第 1 の時刻情報を第 2 の時刻情報として記録する第 2 の時刻情報記録手段と、

前記第 1 の時刻情報を、前記コンテンツ送出手段から送出する前記コンテンツに付加する第 1 の時刻情報付加手段と、

前記第 2 の時刻情報を、前記コンテンツ送出手段から送出する前記コンテンツに付加する第 2 の時刻情報付加手段と、  
を備え、

前記端末装置は、  
前記コンテンツを利用するコンテンツ利用手段と、  
前記コンテンツに付加された少なくとも前記第 1 の時刻情報と第 2 の時刻情報とを、前記コンテンツ利用手段で利用した利用実績として取得し、前記第 1 の時刻情報と前記第 2 の時刻情報とから前記コンテンツの利用部分を特定可能な相対時刻情報を算出し、前記相対時刻情報を記録する相対時刻情報記録手段と、

少なくとも前記相対時刻情報を前記利用実績収集サーバに送信する利用実績送信手段と、  
を備え、

前記利用実績収集サーバは、  
前記端末装置から少なくとも前記相対時刻情報を取得する時刻情報取得手段を

備える

ことを特徴とするコンテンツ利用実績収集システム。

【請求項 3】 端末装置にコンテンツを配信するコンテンツ配信サーバと、前記コンテンツを利用した利用実績を記録し、前記利用実績を利用実績収集サーバに送信する端末装置と、前記端末装置から前記コンテンツの前記利用実績を収集する利用実績収集サーバと、から構成されるコンテンツ利用実績収集システムであって、

前記コンテンツ配信サーバは、

前記コンテンツを送出するコンテンツ送出手段と、

第 1 の時刻情報を生成する第 1 の時刻情報生成手段と、

前記コンテンツの先頭における前記第 1 の時刻情報を第 2 の時刻情報として記録する第 2 の時刻情報記録手段と、

前記第 1 の時刻情報と前記第 2 の時刻情報とから、前記コンテンツの利用部分を特定可能な相対時刻情報を生成し、少なくとも前記相対時刻情報を、前記コンテンツ送出手段から送出する前記コンテンツに付加する相対時刻情報付加手段と、

を備え、

前記端末装置は、

前記コンテンツを利用するコンテンツ利用手段と、

少なくとも前記コンテンツに付加された前記相対時刻情報を、前記コンテンツ利用手段で利用した前記コンテンツの利用実績として記録する相対時刻情報記録手段と、

少なくとも前記相対時刻情報を前記利用実績収集サーバに送信する利用実績送信手段と、

を備え、

前記利用実績収集サーバは、

前記端末装置から少なくとも前記相対時刻情報を取得する相対時刻情報取得手段を備える

ことを特徴とするコンテンツ利用実績収集システム。

【請求項 4】 前記コンテンツ配信サーバはさらに、前記コンテンツを暗号化するコンテンツ暗号化手段を備え、

前記端末装置はさらに、前記暗号化されたコンテンツを復号するコンテンツ復号手段を備える

ことを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載のコンテンツ利用実績収集システム。

【請求項 5】 前記コンテンツ配信サーバはさらに、少なくとも、前記第 1 の時刻情報または前記相対時刻情報を、前記コンテンツにセキュアにバインドするセキュア関連付け手段を備える

ことを特徴とする請求項 4 記載のコンテンツ利用実績収集システム。

【請求項 6】 前記セキュア関連付け手段は、少なくとも、前記第 1 の時刻情報または前記相対時刻情報を、前記コンテンツの暗号化部分に挿入する

ことを特徴とする請求項 5 記載のコンテンツ利用実績収集システム。

【請求項 7】 前記セキュア関連付け手段は、少なくとも、前記第 1 の時刻情報または前記相対時刻情報と、前記コンテンツの暗号化部の平文の一部または全部とのハッシュ値を、前記コンテンツの非暗号化部に設定する

ことを特徴とする請求項 5 記載のコンテンツ利用実績収集システム。

【請求項 8】 前記セキュア関連付け手段は、少なくとも、前記第 1 の時刻情報または前記相対時刻情報と、前記コンテンツの暗号化部の平文の一部または全部とのハッシュ値を、前記コンテンツの暗号化部に設定する

ことを特徴とする請求項 5 記載のコンテンツ利用実績収集システム。

【請求項 9】 前記セキュア関連付け手段は、少なくとも、前記第 1 の時刻情報または前記相対時刻情報と、前記コンテンツの暗号鍵とを関連づけて新たな暗号鍵を生成し、前記コンテンツ暗号化手段は、前記新たな暗号鍵を用いて、前記コンテンツを暗号化する

ことを特徴とする請求項 5 記載のコンテンツ利用実績収集システム。

【請求項 10】 前記セキュア関連付け手段は、少なくとも、前記第 1 の時刻情報または前記相対時刻情報を、前記コンテンツ暗号化手段における入力パラメータとする

ことを特徴とする請求項 5 記載のコンテンツ利用実績収集システム。

【請求項 11】 前記第 1 の時刻情報付加手段が、前記コンテンツに付加する前記第 1 の時刻情報は、MPEG-2 TS (Transport Stream) のPCR (Program Clock Reference) であることを特徴とする請求項 1 または請求項 2 に記載のコンテンツ利用実績収集システム。

【請求項 12】 前記第 1 の時刻情報付加手段が、前記コンテンツに付加する前記第 1 の時刻情報は、PES (Packetized Elementary Stream) のPTS (Presentation Time Stamp) またはDTS (Decoding Time Stamp) であることを特徴とする請求項 1 または請求項 2 に記載のコンテンツ利用実績収集システム。

【請求項 13】 前記第 1 の時刻情報付加手段が前記コンテンツに付加する前記第 1 の時刻情報、または、前記相対時刻情報付加手段が前記コンテンツに付加する前記相対時刻情報は、PES またはMPEG-2 TS のプライベートデータ部に設定されることを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載のコンテンツ利用実績収集システム。

【請求項 14】 前記時刻情報付加手段が前記コンテンツに付加する第 2 の時刻情報は、PES またはMPEG-2 TS のプライベートデータ部に設定されることを特徴とする請求項 2 記載のコンテンツ利用実績収集システム。

【請求項 15】 前記コンテンツ復号手段または前記コンテンツ利用手段は、前記ハッシュ値のチェックにより、前記第 1 の時刻情報または前記第 2 の時刻情報または前記相対時刻情報の改ざんを検出した場合には、前記暗号化されたコンテンツの復号を許可しないことを特徴とする請求項 7 または請求項 8 に記載のコンテンツ利用実績収集システム。

【請求項 16】 前記コンテンツ復号手段または前記コンテンツ利用手段は、

前記ハッシュ値のチェックにより、前記第1の時刻情報または前記第2の時刻情報または前記相対時刻情報の改ざんを検出した場合には、前記第1の時刻情報記録手段または前記相対時刻情報記録手段に対して改ざんされた旨を示す利用実績の取得を指示する

ことを特徴とする請求項7または請求項8に記載のコンテンツ利用実績収集システム。

【請求項17】 前記コンテンツ利用手段は、前記コンテンツのデコードに失敗した場合、前記第1の時刻情報記録手段または前記相対時刻情報記録手段に対して、利用実績を記録しないように指示する

ことを特徴とする請求項9または請求項10に記載のコンテンツ利用実績収集システム。

【請求項18】 前記コンテンツ利用手段は、前記コンテンツのデコードに失敗した場合、前記第1の時刻情報記録手段または前記相対時刻情報記録手段に対して、デコードの失敗を示す利用実績を記録するように指示する

ことを特徴とする請求項9または請求項10に記載のコンテンツ利用実績収集システム。

【請求項19】 前記第1の時刻情報記録手段または前記相対時刻情報記録手段は、前記コンテンツの特殊再生が行われた場合には、利用実績を記録しないことを特徴とする請求項1から請求項3のいずれか1項に記載のコンテンツ利用実績収集システム。

【請求項20】 前記第1の時刻情報記録手段または前記相対時刻情報記録手段は、前記コンテンツの特殊再生が行われた場合には、特殊再生が行われた旨を示す利用実績を記録する

ことを特徴とする請求項1から請求項3のいずれか1項に記載のコンテンツ利用実績収集システム。

【請求項21】 前記コンテンツ復号手段は、前記第1の時刻情報または前記相対時刻情報を取得する間隔により、前記コンテンツの特殊再生が行われていることを検出する

ことを特徴とする請求項19または請求項20に記載のコンテンツ利用実績収集

システム。

【請求項 22】 前記コンテンツ利用手段は、前記コンテンツの特殊再生が行われた場合に、前記第 1 の時刻情報記録手段または前記相対時刻情報記録手段に対して、特殊再生が行われたことを通知する

ことを特徴とする請求項 19 または請求項 20 に記載のコンテンツ利用実績収集システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信や放送を用いて、サーバ装置から映像、音楽などのデジタルコンテンツを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの利用実績を取得し、サーバ装置に利用実績を送信することで、サーバ装置においてユーザのデジタルコンテンツの利用実績を収集可能なシステムおよび装置に関する。

【0002】

【従来の技術】

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。

【0003】

例えば、特許文献 1 ならびに特許文献 2 には、ユーザが端末装置においてコンテンツを再生した回数や時刻、あるいは、コンテンツを記録メディアにコピーした回数や時刻等を利用実績として記録し、定期的に指定されたサーバ装置に利用

実績を送信するシステムが、コンテンツ利用実績収集システムの一例として記載されている。

#### 【0004】

このように、従来のコンテンツ利用実績収集システムでは、ユーザがコンテンツを利用した回数や、コンテンツを利用した時刻等の利用実績を、サーバ装置に送信することができるようになっている。

#### 【0005】

##### 【特許文献1】

特開 2000-564425号公報

#### 【0006】

##### 【特許文献2】

特開 2001-160003号公報

#### 【0007】

##### 【発明が解決しようとする課題】

しかしながら、従来のコンテンツ利用実績収集システムでは、ユーザがコンテンツのどの部分を視聴したかを、コンテンツプロバイダやサービスプロバイダがセキュアに把握、すなわち、改ざんされ得ない状態で取得することはできなかった。

#### 【0008】

特に、MPEG (Moving Picture Experts Group) -2 Systems などのように、コンテンツフォーマットに既存の時刻情報が存在するものの、本来は映像、音声などの複数のストリーム (ES) の同期を確保するために付与されている時刻情報であるため、利用実績の把握のために当該時刻情報を柔軟に変更することができないという課題があった。なお、MPEG-2 Systems は、国際標準である ISO/IEC 13818-1 に規定されている。

#### 【0009】

本発明は、こうした従来の問題点を解決するものであり、コンテンツにセキュアに付与された時刻情報を、コンテンツを利用する端末において利用実績として

記録し、この時刻情報を用いて、コンテンツプロバイダ、サービスプロバイダが、ユーザがコンテンツのどの部分を利用したかを把握し、毎分視聴率、平均視聴率といった重要な情報を得ることが可能なコンテンツ利用実績収集システムを提供することを目的としている。

#### 【0010】

特に、MPEG-2 Systems等、コンテンツフォーマットに既存の時刻情報が存在し、運用等で当該時刻情報を柔軟に変更することがシステムの困難である場合においても、既存のシステムとの親和性が高いコンテンツ利用実績収集システムを提供することを目的としている。

#### 【0011】

さらに、端末装置で特殊再生等がなされている間は利用実績を取得しないようにする制御を行うことによって、ユーザが実際にコンテンツを視聴した部分の利用実績が取得可能なコンテンツ利用実績収集システムを提供することを目的としている。

#### 【0012】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明に関わるコンテンツ利用実績収集システムは、端末装置にコンテンツを配信するコンテンツ配信サーバと、前記コンテンツを利用した利用実績を記録し、前記利用実績を利用実績収集サーバに送信する端末装置と、前記端末装置から前記コンテンツの前記利用実績を収集する利用実績収集サーバとから構成されるコンテンツ利用実績収集システムであって、前記コンテンツ配信サーバは、前記コンテンツを送出するコンテンツ送出手段と、第1の時刻情報を生成する第1の時刻情報生成手段と、前記第1の時刻情報を、前記コンテンツ送出手段から送出する前記コンテンツに付加する第1の時刻情報付加手段と、前記コンテンツの先頭における前記第1の時刻情報を第2の時刻情報として記録する第2の時刻情報記録手段とを備え、前記端末装置は、前記コンテンツを利用するコンテンツ利用手段と、前記コンテンツに付加された少なくとも前記第1の時刻情報を、前記コンテンツ利用手段で利用した前記コンテンツの利用実績として記録する第1の時刻情報記録手段と、前記第1の時刻情報を前記利用

実績収集サーバに送信する利用実績送信手段と、を備え、前記利用実績収集サーバは、前記端末装置から少なくとも前記第1の時刻情報を取得する第1の時刻情報取得手段と、前記コンテンツ配信サーバから少なくとも前記第2の時刻情報を取得する第2の時刻情報取得手段と、前記第1の時刻情報と前記第2の時刻情報とから、前記コンテンツの利用部分を特定可能な相対時刻情報を算出する利用実績取得手段とを備えることを特徴とする。

### 【0013】

#### 【発明の実施の形態】

##### (実施の形態1)

以下、本発明における実施の形態1について、図面を用いて詳細に説明する。

### 【0014】

図1は、本発明における実施の形態1に関わるコンテンツ利用実績収集システム1の全体の概略構成を示す図である。

このコンテンツ利用実績収集システム1は、ネットワークあるいは記録メディア等を通じて配信センター（すなわち、サービスプロバイダ）から配信される暗号化コンテンツを、ユーザが端末装置において利用し、その利用実績を収集するシステムであって、コンテンツ等を配信する配信センター101と、コンテンツを利用する端末装置102a～102cと、これらを相互に接続するネットワーク103とから構成されている。

### 【0015】

配信センター101は、ユーザに対して課金を行うための課金サーバ101aと、ユーザが所有するコンテンツを利用する権利（利用条件）の管理や、コンテンツのライセンスを生成し、端末装置102a～102cに配信を行う権利管理サーバ101bと、コンテンツを配信するコンテンツ配信サーバ101cと、ネットワーク103を通じて端末装置102a～102cに各種サービスを提供するためのウェブ画面を送信するウェブサーバ101dと、端末装置102a～102cから収集した利用実績を管理する利用実績収集サーバ101eとから構成されている。

### 【0016】

課金サーバ101aは、インターネット等を通じて、コンテンツの利用条件等を購入する際に、オンラインでの課金を行うためのサーバ装置である。具体的には、課金サーバ101aは、クレジットカードを用いて課金、決済を行ったり、予め課金サーバ101aにユーザの銀行口座番号を登録しておき、ネットワーク103を経由して端末装置102a～102cからアップロードされた購入の履歴等に基づき、課金、決済を行ったりする。

#### 【0017】

権利管理サーバ101bは、ユーザが所有するコンテンツの利用条件を管理し、ユーザに暗号化されたコンテンツを復号するためのライセンスを付与するサーバ装置である。具体的には、権利管理サーバ101bは、ユーザ毎、あるいは、端末装置102a～102c毎に、それぞれが所有するコンテンツの利用条件を管理しておき、ユーザからの要求に基づき、ネットワーク103を通じて、ライセンスを端末装置102a～102cに配信する。あるいは、デジタル放送やブロードバンド放送等のプッシュ型の配信形態では、一時的に無効化されたライセンスをコンテンツと共に配信し、端末装置102a～102cにおいて課金処理を行うことによりライセンスを有効化し、コンテンツを利用する、というようにすることもできる。

#### 【0018】

なお、コンテンツを暗号化する暗号アルゴリズムは、AES (Advanced Encryption Standard) や Triple DES (Data Encryption Standard) 等の共通鍵暗号アルゴリズムが用いられるのが一般的である。

#### 【0019】

また、ライセンスは、暗号化されたコンテンツを復号するための復号鍵（コンテンツ鍵）と、コンテンツの利用期限や利用回数などの利用条件等から構成されており、ライセンスチケット (License Ticket、以下、LTと記述) と呼ばれるデータである。なお、LTのデータ構造については、後で図を用いて詳細に説明する。

#### 【0020】

LT等のデータを、ネットワーク103を通じて、配信センター101と端末装置102a~102cとの間で送受信する場合には、セキュリティを確保するため、SSL (Secure Socket Layer) などの安全な認証チャネル (Secure Authenticated Channel、以下、SACと記述) を確立してから、データの送受信を行う。

#### 【0021】

コンテンツ配信サーバ101cは、ネットワーク103を通じて端末装置102a~102cにコンテンツを配信するためのサーバ装置であり、ワークステーション等により実現される。具体的には、コンテンツ配信サーバ101cは、MPEG-2やMPEG-4等の圧縮方式によりデジタル圧縮され、必要に応じてAESやTriple DES等により暗号化されたコンテンツをストリーミング配信する。

#### 【0022】

特に、インターネット等のIP (Internet Protocol) を用いたネットワークにおいてストリーミング配信を行う場合は、IETF (Internet Engineering Task Force) によってRFC (Request For Comments) として標準化されているRTP (Realtime Transfer Protocol) およびRTCP (Real Time Control Protocol) が用いられる。

#### 【0023】

RTPは、コンテンツをRTPパケットと呼ばれる可変長のパケットに分割して伝送し、RTPパケットのヘッダには、RTPパケットの並び替えやRTPパケットのロスを検出するために用いられるシーケンス番号、ストリーム中の映像と音声の同期等に用いるタイムスタンプ等の情報が設定できるようになっている。RTPパケットに設定するコンテンツは、MPEG-2やMPEG-4のES (Elementary Stream) でも良いし、MPEG2-TS (Transport Stream) で多重化されたコンテンツでも良い。またRTPは、一般には、UDP (User Datagram Protocol) / IPを下位プロトコルとして用いている。

## 【0024】

R T C Pは、R T Pを制御するためのプロトコルであり、R T Pと対で用いられ、R T Pパケットを受信した際に検出できるパケットロスや遅延ジッタを送出側にフィードバックすることができる。送出側は、このフィードバック情報を用いて、ストリーミングの帯域制御等を行う。

## 【0025】

すなわち、ストリーミング配信では、コンテンツ配信サーバ101cは、端末装置102a～102cからリクエストされたコンテンツを分割して、R T Pヘッダを付加し、R T Pパケットを生成して端末装置102a～102cに順次送出する。端末装置102a～102cでは、受信したR T Pパケットを復元すると共に、R T Pヘッダ内の情報を参照しながら、映像、音声のデコードを行い、モニター等に出力する。この際、R T Pヘッダから取得したパケットロスや遅延ジッタ等を検出し、R T C Pを用いてコンテンツ配信サーバ101cに送信する処理を行う。

## 【0026】

また、コンテンツ配信サーバ101cは、ダウンロード型のコンテンツを配信するシステムであっても良く、この場合、F T P ( F i l e T r a n s f e r P r o t o c o l ) や H T T P ( H y p e r T e x t T r a n s f e r P r o t o c o l ) 等のプロトコルを用いてダウンロードコンテンツを提供するサーバ装置であったりする。また、デジタル放送の場合であれば、M P E G - 2 T Sでストリーム型コンテンツを提供する送出装置であったり、A R I B ( A s s o c i a t i o n o f R a d i o I n d u s t r i e s a n d B u s i n e s s e s ) S T D - B 2 4等 に示されているデータカールセル伝送方式に基づいた蓄積型コンテンツを提供する送出装置であったりする。

## 【0027】

ウェブサーバ101dは、ユーザが端末装置102a～102cから各種サービスにアクセスするためのコンテンツ購入画面等を提供する。具体的には、ウェブサーバ101dは、インターネットを通じて、H T T P等のプロトコルにより、H T M L ( H y p e r T e x t M a r k u p L a n g u a g e ) や X M L

(Extensible Markup Language) 等のスクリプト言語で記述されたウェブページを提供したり、デジタル放送において、BML (Broadcasting Markup Language) で記述されたページを提供したりする。

#### 【0028】

利用実績収集サーバ101eは、端末装置102a～102cにおいて記録された種々の利用実績を収集し、管理するサーバ装置である。具体的には、利用実績収集サーバ101eは、端末装置102a～102cとSSLなどを用いてSACを確立し、HTTP等のプロトコルを用いて、端末装置102a～102cからコンテンツの利用実績を収集する。これらを、データベース等を用いて管理し、毎分視聴率、平均視聴率などの視聴率データとして活用する。

#### 【0029】

LAN101nは、配信センター101において、課金サーバ101aと、権利管理サーバ101bと、コンテンツ配信サーバ101cと、ウェブサーバ101dと、利用実績収集サーバ101eとを相互に接続するためのネットワークである。例えば、IEEE802.3等の有線ネットワークや、IEEE802.11b等の無線ネットワークを用いて実現することができる。

#### 【0030】

ネットワーク103は、配信センター101と端末装置102a～102cとを相互に接続するネットワークである。例えば、ネットワーク103は、インターネット等の通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

#### 【0031】

端末装置102a～102cは、ネットワーク103と接続する機能を有し、ユーザがコンテンツをモニター画面などで利用したり、記録メディアにコンテンツを書き出したりするための端末装置である。具体的には、端末装置102a～102cは、デジタル放送を受信するためのSTB (Set Top Box)、デジタルTV、DVD (Digital Versatile Disc) レコーダ、HDD (Hard Disk Drive) レコーダ、PC (Pers

onal Computer) などのコンテンツ表示装置、レコーダ、あるいは、これらの複合機器である。

#### 【0032】

このようなコンテンツ利用実績収集システム1において、ネットワーク103を通じてコンテンツやライセンスが配信され、端末装置102a～102cにおいてコンテンツを利用すると共にコンテンツの利用実績を記録し、端末装置102a～102cから配信センター101に利用実績を送信する処理を、図2～図25の図面を用いて詳細に説明する。但し、以下では、端末装置102a～102cについては、端末装置102aをその代表とし、端末装置102として説明する。また、端末装置102において、配信センター101の権利管理サーバ101bが端末装置102に対して、LTを用いて利用実績を収集する指示を行う場合の例を示す。

#### 【0033】

図2は、図1に示される配信サーバ101における権利管理サーバ101bの詳細な構成を示す機能ブロック図である。

権利管理サーバ101bは、大きく分けて、HDD等に格納されたデータファイル等によって実現されるデータベース部200と、LSI等のハードウェアあるいはCPU、RAM、ROM等を利用して実行されるプログラム等によって実現されるライセンス処理部210とから構成されている。データベース部200は、ユーザ情報DB201、コンテンツ鍵DB202、利用条件DB203、利用実績収集条件DB204とから構成され、ライセンス処理部210は、利用実績収集指示手段211、ライセンス発行手段212、第1の送受信手段213とから構成される。

#### 【0034】

まず、データベース部200の各々の手段について詳細に説明する。

ユーザ情報DB201は、ユーザに関する情報を管理するためのユーザ情報管理テーブルを有するデータベースであって、権利管理サーバ101bにアクセスする端末装置102と、利用条件DB203で管理されるコンテンツの利用条件を所有するユーザとを関連付けるために用いられる。

**【0035】**

具体的には、ユーザ情報DB201は、図3に示すユーザ情報管理テーブル300を有し、コンテンツ利用実績収集システム1内でユーザを一意に特定するためのユーザID301と、コンテンツ利用実績収集システム1内で端末装置102を一意に特定するための端末ID302と、ユーザに関する詳細情報を示すユーザプロフィール303と、利用実績の収集に関するユーザのポリシーを示すプライバシーポリシー304とを管理している。

**【0036】**

ここで、ユーザプロフィール303とは、ユーザの名前、年齢、性別、住所や、ユーザの好みの番組、趣味等のユーザ登録情報のことを示しており、利用実績を収集するユーザを決定したり、ユーザの好みの番組と利用実績を収集した番組との関連性から、ユーザのコンテンツの利用傾向を分析したりするための判断材料に用いることができる。

**【0037】**

また、プライバシーポリシー304とは、ユーザがサービスプロバイダに対して、コンテンツの利用実績の全部または一部を提供することを承諾するか否かを示す情報のことであり、ユーザのプライバシーに対する意向に沿った利用実績を実現するためのものである。

**【0038】**

例えば、図3において、ユーザID301が「USER-ID-00001」であるユーザは、端末ID302が「TERMINAL-ID-00001」である端末装置102を所有していることを示している。また、ユーザプロフィール303からは、ユーザ「USER-ID-00001」は、「男性、31歳」であることが分かり、プライバシーポリシー304が「実績収集OK」となっていることから、ユーザ「USER-ID-00001」は、端末装置102において利用したコンテンツの利用実績の収集を許可していることを示している。ここで、利用実績とは、ユーザが端末装置102において利用したコンテンツ中の再生箇所や、早送り、巻き戻しといった特殊再生に関する情報等、ユーザの詳細な操作内容等を表すものとする。

## 【0039】

また、ユーザID301が「USER-ID-00002」であるユーザは、端末ID302が「TERMINAL-ID-12345」、「TERMINAL-ID-54321」という2つの端末装置102を有しており、両方の端末装置102から権利管理サーバ101bにアクセス可能であることを示している。

## 【0040】

また、ユーザ「USER-ID-00002」のプライバシーポリシー304についても、「実績収集OK」となっていることから、端末装置102におけるコンテンツの利用実績の収集を許可することを示している。これに対して、ユーザID301が「USER-ID-00004」であるユーザのプライバシーポリシー304は、「実績収集NG」となっていることから、サービスプロバイダによるコンテンツの利用実績の収集を承諾しない設定になっていることが分かる。

## 【0041】

なお、ユーザ情報DB201へのデータ登録は、ユーザによって、サービスプロバイダが提供するサービスを受けるために会員登録をする際に行なわれる。この会員登録処理は、ユーザがネットワーク103を通じてウェブサーバ101dが提供する会員登録画面により、配信センター101と端末装置102とがオンラインで行っても良いし、会員登録用の葉書を用いる等、オフラインで行っても良い。会員登録処理では、まずサービスプロバイダがユーザに対してユーザID301を割り当てる。その後、ユーザが所有する端末装置102の端末ID302が、オンラインまたはオフラインによりサービスプロバイダに通知されるので、ユーザID301と端末ID302とが関連付けられて、ユーザ情報DB201のユーザ情報管理テーブル300に登録される。以上のような会員登録処理を行った結果、ユーザ情報DB201が構築される。

## 【0042】

コンテンツ鍵DB202は、暗号化コンテンツを復号するためのコンテンツ鍵を管理するデータベースであって、端末装置102からのライセンス取得要求（LT取得要求）に対してLTを生成する際に、LT取得要求に含まれるコンテン

コンテンツIDに対応したコンテンツ鍵を取得するために用いられる。

#### 【0043】

具体的には、コンテンツ鍵DB202は、図4に示すように、コンテンツ利用実績収集システム1においてコンテンツを一意に識別するコンテンツID401と、コンテンツID401に対応するコンテンツ鍵402とからなるコンテンツ鍵管理テーブル400を有する。

#### 【0044】

例えば、コンテンツID401が「CONTENT-ID-00001」の暗号化コンテンツを復号するためのコンテンツ鍵402が「0x1234567890abcdef」であることを示している。

#### 【0045】

利用条件DB203は、ユーザ毎のコンテンツに対する利用条件を管理するデータベースであって、端末装置102からのLT取得要求に対して、ユーザが所有する利用条件を満たすか否かを判定し、利用条件を満たす場合にLTを生成するために用いられる。

#### 【0046】

具体的には、利用条件DB203は、図5に示すように、コンテンツ利用実績収集システム1においてユーザを一意に識別し、利用条件の所有者を示すユーザID501と、ユーザID501に示されるユーザが所有する利用条件を識別するための利用条件ID502と、コンテンツ利用実績収集システム1においてコンテンツを一意に識別し、利用条件が利用を許諾するコンテンツのコンテンツID503と、コンテンツID503で示されるコンテンツの利用が可能となる開始、終了日時を示す有効期間504と、コンテンツID503で示されるコンテンツの利用可能な回数を示す利用可能回数505とからなる利用条件管理テーブル500を有する。

#### 【0047】

例えば、ユーザID501が「USER-ID-00001」であるユーザは、利用条件ID502が「URUs-ID-00001」なる利用条件を保持している。利用条件「URUs-ID-00001」は、利用を許諾するコンテン

ツがコンテンツID503に示される「CONTENT-ID-00001」なるコンテンツであり、有効期間504は「2002/12/31~2003/1/30」であり、利用可能回数505は無制限(∞)、すなわち、何回でも利用可能であることを示している。また、ユーザID501が「USER-ID-00002」であるユーザは、利用条件ID502が「URUs-ID-00002」と「URUs-ID-10011」という2つの利用条件を有している。このうち、利用条件「URUs-ID-00002」は、コンテンツID503が「CONTENT-ID-13452」なるコンテンツに対する利用条件であり、有効期間504が「2002/12/1~2002/12/31」、利用可能回数505が「5回」であるので、有効期間内で最大5回まで当該コンテンツを利用可能であることを示している。また、利用条件「URUs-ID-10011」は、コンテンツID503が「CONTENT-ID-99999」なるコンテンツの利用条件であり、有効期間504は無制限(∞)であるが、利用可能回数505に示されるように、コンテンツを利用可能な回数は「1回」のみであることを示している。

#### 【0048】

利用実績収集条件DB204は、端末装置102に対して利用実績の収集を指示するための条件を管理するデータベースであり、コンテンツ毎に、どのユーザから利用実績を収集するかといった条件や、端末装置102において利用実績を記録するタイミング、端末装置102から利用実績収集サーバ101eに利用実績を送信するタイミング、記録する利用実績の内容等を管理し、端末装置102に対して利用実績を収集するように指示を行う場合に用いられる。

#### 【0049】

具体的には、利用実績収集条件DB204は、図6に示すように、コンテンツ利用実績収集システム1内でコンテンツを一意に識別するコンテンツID601と、利用実績を収集するユーザを決定するための条件、および、利用実績の収集タイミングや利用実績の内容に関する条件を示す利用実績収集条件602とからなる利用実績収集条件管理テーブル600を有する。利用実績収集条件602は、利用実績を収集するユーザを決定するための条件を示す対象ユーザ決定条件6

03と、利用実績を記録するための条件を示す利用実績記録条件604と、記録する利用実績の項目（内容）を示す利用実績内容605と、記録した利用実績を端末装置102から利用実績収集サーバ101eに送信する条件を示す利用実績返却条件606とを含んでいる。

#### 【0050】

例えば、コンテンツID601が「CONTENT-ID-00001」のコンテンツは、対象ユーザ決定条件603に示されるように、利用実績を収集するユーザあるいは端末装置102が「ランダム」に決定される。また、利用実績記録条件604は「コンテンツ単位」と設定されている。これは、ユーザがコンテンツを利用する単位で利用実績を取得することを示しており、例えば、コンテンツ利用開始時に利用実績を記録するような場合などである。利用実績内容605は、「アクション、時刻」であるので、コンテンツの再生、コピーなどのユーザの操作（アクション）の内容と、ユーザの操作が行われた時刻を記録する。さらに、利用実績返却条件606は「毎日5：00」となっているので、記録した利用実績を、毎日5：00に利用実績収集サーバ101eに送信することを指示している。以上のように、コンテンツ「CONTENT-ID-00001」に関する利用実績収集条件602は、利用実績を収集する対象となるユーザをユーザ情報DB201から「ランダム」に決定し、決定されたユーザに対して、「コンテンツ単位」に「アクション」とアクションが実行された「時刻」を記録するように指示し、記録された利用実績を「毎日5：00」に利用実績収集サーバ101eに送信する、というものである。ここで、利用実績を収集するユーザをランダムに決定する方法としては、例えば、一様乱数等を用いて乱数を発生させ、この乱数に対応するユーザ情報DB201のユーザ情報管理テーブル300のユーザID301（例えば、「USER-ID」に続く5桁の番号を用いる等）に該当するユーザを選択する方法が考えられる。

#### 【0051】

また、コンテンツID601が「CONTENT-ID-00002」であるコンテンツに関しては、対象ユーザ決定条件603で「全ユーザ」と示されているように、コンテンツ「CONTENT-ID-00002」のLTを発行する

全てのユーザが、利用実績を収集する対象ユーザとして決定される。また、利用実績記録条件604では、「ユーザ操作単位、特殊再生あり」とあるように、利用実績として「ユーザ操作単位」、つまり、ユーザが利用操作（例えば、再生、停止、ポーズ、早送り、等）を行う都度、利用実績を記録するよう指示している。また、利用実績内容605は「利用部分」とあるように、ユーザがコンテンツのどの部分を利用したかを、特殊再生部分も含めて詳細に記録するよう指示している。さらに、利用実績返却条件606は、「ユーザ操作ごと」とあるように、1または複数のユーザ操作を行った時点で、端末装置102から利用実績収集サーバ101eに利用実績が送信される。

#### 【0052】

さらに、コンテンツID601が「CONTENT-ID-00003」であるコンテンツでは、対象ユーザ決定条件603は「プライバシーポリシー」となっているので、ユーザ情報DB201を参照することにより、ユーザのプライバシーポリシーに応じて、利用実績の収集の対象ユーザとするか否かが決定される。このコンテンツ「CONTENT-ID-00003」の利用実績記録条件604では、「ユーザ操作単位、特殊再生除外」を収集するように指定されており、利用実績として「ユーザ操作単位」、つまり、ユーザが利用操作の都度、利用実績を記録するよう指示しているが、早送り、巻戻しなどの特殊再生についての利用実績は除外するよう指示している。また、利用実績内容605は「アクション、時刻、利用部分」とあるように、ユーザの操作内容と、ユーザ操作が行われた時刻（絶対時刻）を記録すると共に、ユーザがコンテンツのどの部分を視聴したかを、特殊再生部分を除いて詳細に記録するよう指示している。

#### 【0053】

なお、コンテンツ「CONTENT-ID-00003」の利用実績返却条件606は、「コンテンツ利用直後」となっているので、コンテンツの利用を終了した時点で、端末装置102から利用実績収集サーバ101eに対して利用実績を送信するよう指示する例を示している。

#### 【0054】

また、コンテンツ「CONTENT-ID-00004」では、対象ユーザ決

定条件 603 に「UR10 権利以上」と指定されており、利用条件 DB 203 中に、利用条件を 10 レコード以上所有しているユーザに対してのみ、利用実績の収集を行うように指示している。また、利用実績返却条件 606 では、「LT 返却時」として指定されており、1 または複数の LT を返却するタイミングと同期させて、利用実績を収集するよう指示している。

#### 【0055】

以上、データベース部 200 の各々の手段についての詳細な説明を行った。

次に、ライセンス処理部 210 の各々の手段についての詳細な説明を行う。

利用実績収集指示手段 211 は、端末装置 102 に対して、利用実績の収集を指示するための指示情報を生成する手段である。

#### 【0056】

具体的には、利用実績収集指示手段 211 は、ユーザからの LT 発行要求を受けた場合に、必要に応じて、ユーザ情報 DB 201、利用条件 DB 203、利用実績収集条件 DB 204 等を用いて、利用実績の収集のための指示情報を生成し、LT に設定するためにライセンス発行手段 212 に指示情報を送信する。

#### 【0057】

ライセンス発行手段 212 は、端末装置 102 からの LT 発行要求に応じて、LT を生成するための手段である。

具体的には、ライセンス発行手段 212 は、端末装置 102 からの LT 発行要求を受け、ユーザ情報 DB 201 と、コンテンツ鍵 DB 202 と、利用条件 DB 203 とを利用し、LT 発行要求がユーザの利用条件を満たすか否かを判定した上で、LT を生成する処理を行う。また、権利管理サーバ 101b から端末装置 102 に対して、ユーザのコンテンツの利用実績の収集を指示するため、利用実績収集指示手段 211 から利用実績の収集のための指示情報を受け取り、LT に設定する。

#### 【0058】

第 1 の送受信手段 213 は、ネットワーク 103 を通じて、端末装置 102 と通信するための手段である。

以上、権利管理サーバ 101b の詳細な構成について、説明を行った。

**【0059】**

ここで、ライセンス発行手段212が生成するLT、および、利用実績収集指示手段211が生成する利用実績の収集のための指示情報の構成を、図7～図8を用いて詳細に説明する。

**【0060】**

図7は、LTの構成の一例を示す図である。図7に示すLT700は、LT700が利用を許諾するコンテンツのコンテンツIDやLT700の有効期限等を含むLTヘッダ701、コンテンツの再生や、記録メディアへのコピーが可能な回数等の利用条件を示すLTアクションタグブロック702、コンテンツを復号するためのコンテンツ鍵を含むコンテンツ鍵タグブロック703、権利管理サーバ101bから端末装置102に対して利用実績の収集を指示するための利用実績収集指示タグブロック704、LT700の改ざんを検出するためのハッシュ値であるLTフッタ705とから構成されている。

**【0061】**

LTヘッダ701は、LT700を識別するためのLT識別子711、ユーザ毎またはシステム毎でLT700を一意に特定可能な識別子であるライセンスID712、LT700全体の長さを示すLTサイズ713、LT700が利用を許諾するコンテンツの識別子であるコンテンツID714、LT700が利用可能な期間を示すLT有効期間715から構成される。

**【0062】**

LTアクションタグブロック702は、「再生」、「コピー」、「印刷」等の、コンテンツに対するユーザのアクションを特定するためのアクションID721と、アクションの実行が許諾される回数を示す回数カウンタ722と、コンテンツの再生、コピー等を行う手段に固有な利用条件を示す利用手段固有条件723とから構成される。ここで、利用手段固有条件723とは、端末装置102におけるコンテンツを利用するための手段の種類や性能に依存する利用条件である。例えば、映画コンテンツの音声チャンネルの指定（5.1chで再生可能か、2chで再生可能か）や、画像コンテンツの解像度、サイズの指定等が挙げられる。

**【0063】**

コンテンツ鍵タグブロック 703 は、暗号化コンテンツを復号するためのコンテンツ鍵がバイナリ値で設定される。

利用実績収集指示タグブロック 704 は、利用実績収集指示手段 211 において生成されるタグブロックであり、図 8 に示すフォーマットを有する。

**【0064】**

ここで、図 8 を用いて、利用実績収集タグブロック 804 の詳細な構成について説明する。

利用実績収集指示タグブロック 704 は、利用実績収集指示タグブロック 704 を識別するための識別子である利用実績収集指示タグ値 801、利用実績収集指示タグブロック 704 の長さを示す指示情報長 802、利用実績の収集を指示する情報である指示情報 803 とから構成される。

**【0065】**

指示情報 803 は、利用実績記録条件 811 と、利用実績内容 812 と、利用実績返却条件 813 とから構成されている。ここでは、利用実績記録条件 811 として、「ユーザ操作単位、特殊再生除外」は、特殊再生を除くユーザのコンテンツを利用する操作の単位で利用実績を記録する指示を、利用実績内容 812 の「アクション」および「時刻」および「利用部分」は、ユーザがコンテンツを利用する動作の内容（例えば、再生、コピー等）を示すアクションと、そのアクションが行われた絶対時刻を記録する指示を、利用実績返却条件 813 の「コンテンツ利用直後」は、当該コンテンツの利用を終了した直後に、利用実績収集サーバ 101e に利用実績を送信する指示を表している。

**【0066】**

なお、利用実績内容 812 において「時刻」が指定された場合のため、端末装置 102 において、コンテンツを利用した絶対時刻を記録するための、セキュアな計時手段を有するようにしても良い。

**【0067】**

以上、図 8 を用いて、利用実績収集タグブロック 804 の詳細な構成についての説明を行った。以下、図 7 を用いて、LT700 についての説明を継続する。

LTフッタ705は、LT700をハードディスク等の非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、LTの内容が更新される度に、LT700のハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパされたエリアで管理される必要がある。具体的なハッシュアルゴリズムとしては、SHA-1 (Secure Hash Algorithm 1) や、SHA-256等を用いることができる。

#### 【0068】

以上、図7～図8を用いて、LT700と利用実績の収集のための指示情報である利用実績収集指示タグブロック704について、その詳細な構成の説明を行ったことにより、ライセンス処理部210の各々の手段についての詳細な説明を終了する。

#### 【0069】

次に、図9は、図1に示される配信サーバ101におけるコンテンツ配信サーバ101cの詳細な構成を示す機能ブロック図である。

コンテンツ配信サーバ101cは、端末装置102からのコンテンツ取得要求に応じて、MPEG-2、MPEG-4等のコンテンツをMPEG-2 TSで出力する装置であって、コンテンツ取得要求受信手段901と、コンテンツ取得手段902と、コンテンツDB903と、コンテンツ多重化手段904と、コンテンツ暗号化手段905と、コンテンツ鍵供給手段906と、計時手段907と、第1の時刻情報付加手段908と、第2の時刻情報記録手段909と、コンテンツ送出手段910と、コンテンツ鍵DB911とから構成される。

#### 【0070】

コンテンツ取得要求受信手段901は、端末装置102からのコンテンツ送出要求やコンテンツ停止要求を受信し、コンテンツ取得手段902に通知する。具体的には、コンテンツ取得要求受信手段901は、RTSP (Realtime Transport Streaming Protocol) による再生指示 (PLAY) を受信すると、コンテンツ取得手段902に当該コンテンツの取得指示を送信することにより、コンテンツ配信サーバ101cからコンテンツの

送出を開始する。また、端末装置 102 から RTSP によるコンテンツ停止要求 (TEARDOWN) を受信した場合には、コンテンツ取得手段 902 に当該コンテンツの取得停止指示を送信することにより、コンテンツ配信サーバ 101c からコンテンツの送出を停止する。さらに、RTSP による一時停止 (PAUSE) などの特殊再生に対する要求等も処理することができる。

#### 【0071】

コンテンツ取得手段 902 は、端末装置 102 から要求されたコンテンツをコンテンツ DB 903 から読み出し、端末装置 102 に送信する手段である。

具体的には、コンテンツ取得手段 902 は MPEG ストリームを生成するリアルタイムエンコーダであって、コンテンツ取得要求受信手段 901 からの指示に応じて、コンテンツ DB 903 から映像、音声などを読み出し、映像、音声、データなどの MPEG-2 や MPEG-4 の ES を生成する。さらに、これらの ES を含む PES (Packetized Elementary Stream) パケットを生成し、コンテンツ多重化手段 904 に送出する。

#### 【0072】

ここで、図 10 を用いて、PES パケットの構成の概要について説明する。図 10 に示す PES パケット 1000 は、PES パケットの開始を示すコードである Packet Start Code Prefix 1000 と、PES に含まれる音声、映像等のデータの種別を示す Stream id 1020 と、PES パケット 1000 の長さを示す PES Packet Length 1030 と、オプションの PES ヘッダである Optional PES Header 1040 と、スタッフィングである Stuffing Bytes 1050 と、音声、映像等のデータ (ES) が設定される PES Packet Data Bytes 1060 とから構成される。

#### 【0073】

以下、図 9 に戻って、コンテンツ配信サーバ 101c の構成についての説明を継続する。

コンテンツ DB 903 は、コンテンツを蓄積するためのデータベース手段である。具体的には、コンテンツ DB 903 は、例えば、映画、ドキュメンタリーな

どを蓄積するVCR (Video Cassette Recorder) などであったり、ライブ放送 (生放送) 時であれば、映像、音声を撮影するためのビデオカメラであったりする。

#### 【0074】

コンテンツ多重化手段904は、コンテンツ取得手段902から受け取った映像、音声、データ等のコンテンツを多重化し、コンテンツ暗号化手段905に送出する手段である。具体的には、コンテンツ多重化手段904は、PES形式のコンテンツをMPEG-2 TSパケット (以下、TSパケットと記述) に多重化してトランスポートストリームを生成する。

#### 【0075】

図11は、TSパケットの構成の概要を示す図である。TSパケット1100は、TSパケット1100の開始を示すコードやTSパケットに設定されるデータの種類などを特定するためのPID (Packet ID) などが含まれるTSパケット1100のヘッダであるTSP Header1110と、オプション的に用いられ、時刻情報やプライベートデータなどが設定可能なAdaptation Field1120と、PESパケット1000や、PSI (Program Specific Information) / SI (Service Information) などが設定されるペイロードであるTSP Payload1130とから構成される。

#### 【0076】

コンテンツ多重化手段904は、このように生成したトランスポートストリーム (TSパケット1100) を、コンテンツ暗号化手段905に送出する。

コンテンツ暗号化手段905は、AESを用いてコンテンツを暗号化する手段である。具体的には、コンテンツ暗号化手段905は、図11に示すTSパケット1100のAdaptation Field1120を除くペイロード部 (TSP Payload1130) を、コンテンツ鍵供給手段906から取得したコンテンツ鍵 (暗号鍵) を用いて、CBC (Cipher Block Chain) モードによって暗号化する。

#### 【0077】

コンテンツ鍵供給手段 906 は、コンテンツを暗号化するためのコンテンツ鍵をコンテンツ鍵 DB 911 から取得し、コンテンツ暗号化手段 905 に提供する手段である。

#### 【0078】

コンテンツ鍵 DB 911 は、コンテンツを暗号化するためのコンテンツ鍵を管理するデータベースであって、端末装置 102 からの要求に応じて、コンテンツ ID に対応したコンテンツ鍵をコンテンツ鍵供給手段 906 に提供する。コンテンツ鍵 DB 911 が管理するテーブル構成の一例としては、図 4 に示した、権利管理サーバ 101b におけるコンテンツ鍵 DB 202 のコンテンツ鍵テーブル 400 と同様で良いので、ここでは説明を省略する。

#### 【0079】

なお、コンテンツ鍵 DB 911 で管理されるコンテンツ毎のコンテンツ鍵と、権利管理サーバ 101b におけるコンテンツ鍵 DB 202 で管理されるコンテンツ毎のコンテンツ鍵（すなわち、LT 700 に設定される、コンテンツを復号するための鍵）は、一貫性が保たれるように管理されることは言うまでもない。

#### 【0080】

計時手段 907 は、コンテンツ配信サーバ 101c 内での基準となる時刻を出力する手段である。具体的には、計時手段 907 は、STC (System Time Clock) と呼ばれる 27MHz の精度を有する 42 ビットの基準時刻を生成して、第 1 の時刻情報付加手段 908 に供給する。

#### 【0081】

第 1 の時刻情報付加手段 908 は、計時手段 907 から第 1 の時刻情報を取得し、コンテンツ取得手段 902 およびコンテンツ多重化手段 904 に対して第 1 の時刻情報を付加する手段である。具体的には、第 1 の時刻情報付加手段 908 は、計時手段 907 から STC の値を取得して、コンテンツ取得手段 902 に対して、MPEG-2 Systems の規約に従い、少なくとも 700ms の精度で PTS および DTS のためのタイムスタンプを付与する。また、コンテンツ多重化手段 904 に対しては、MPEG-2 Systems の規約に従い、少なくとも 100ms の精度で PCR のためのタイムスタンプを付与する。

**【0082】**

すなわち、コンテンツ取得手段902は、第1の時刻情報付加手段908から取得した第1の時刻情報、すなわちSTCの値を用いて、PESパケット1000を生成する際、Optional PES Header 1040中の、Optional Fields 1043の要素であるPTS (Presentation Time Stamp) 1043a、DTS (Decoding Time Stamp) 1043bをPESパケット1000に付加する。

**【0083】**

PTS 1043aは、当該PESパケット1000に含まれる映像、音声等を端末装置102a~102cにおいて表示する時刻を示す情報である。また、DTS 1043bは、当該PESパケット1000に含まれる映像、音声等をデコードする時刻を示す情報である。

**【0084】**

これらのPTS 1043aおよびDTS 1043bは、端末装置102a~102cにおいて、端末装置102a~102cが保持するSTCと一致する毎に、個々のPESパケットのデコード、表示を確実に行えるよう、適切なPESパケット1000に設定される。

**【0085】**

また、コンテンツ多重化手段904についても、第1の時刻情報付加手段908から取得した第1の時刻情報(STC)の値を用いて、TSパケット1100を生成する際、TSパケット1100のAdaptation Field 1120のOptional Fields 1125内の要素であるPCR (Program Clock Reference) 1125aを付加する。端末装置102a~102cは、このPCR 1125aを用いて、複数のES (映像、音声、データ等)を同期させる際の基準となり、送信装置のSTCと同期した基準クロック(STC)を再生することが可能となる。

**【0086】**

ここで、PCR 1125aに付加した第1の時刻情報は、端末装置102において、ユーザがコンテンツのどの部分を利用したかを記録するために用いられる

が、PCR1125aはTSパケット1100の非暗号化部に存在するため、PCR1125aの値が不正に改ざんされ、配信センター101において正しい利用実績が取得できない恐れがある。ゆえに、コンテンツ多重化手段904において、少なくともPCR1125aと、コンテンツ暗号化手段905において暗号化されるTSP Payload1130とのハッシュを計算して、TSパケット1100のPrivate Data1125eに設定する。すなわち、コンテンツ多重化手段904は、第1の時刻情報とコンテンツとをセキュアにバインドする手段であるとも言える。

#### 【0087】

なお、Private Data Length1125dは、追加したハッシュ値の長さに応じて、適切な値が設定される。本実施の形態では、Adaptation Field1120とTSP Payload1130のハッシュを計算して、Private Data1125eに設定する場合を考える。なお、TSパケット1100のどの部分のハッシュを計算するかについては、少なくとも、第1の時刻情報であるPCR1125aと、コンテンツ暗号化手段905と端末装置102のコンテンツ復号手段1521との間で共有される何らかの秘密情報とであれば、本実施の形態に限られるものではない。また、第1の時刻情報は、上記PCR1125aに限られるものではなく、例えば、プライベートデータ部（Private Data1125e）に設定された時刻情報などであっても良い。

#### 【0088】

また、第1の時刻情報付加手段908がコンテンツ（番組）の開始時点でのPCR1125aの値を取得するため、例えば、コンテンツ取得手段902においてTSパケット1100のPrivate Data1125eに、コンテンツの開始（先頭）を示すフラグを設定するようにしておくようにすれば、第1の時刻情報付加手段908は、上記フラグを検出した時点でのPCR1125aの値（すなわち、STCの値）を第2の時刻情報として取得することで、第2の時刻情報記録手段909に送信することができる。なお、図9には図示しない上流システム（例えば、番組運行管理システム、等）から、コンテンツ開始のタイミン

グを受け取るようにしても良い。

#### 【0089】

第2の時刻情報記録手段909は、第1の時刻情報付加手段908から取得した、第2の時刻情報を記録する手段である。この第2の時刻情報は、利用実績の記録のため、必要に応じて、LAN101nを通じて利用実績収集サーバ101eに送信される。

#### 【0090】

コンテンツ送出手段910は、コンテンツ暗号化手段905において暗号化されたTSパケットを、端末装置102に送出する手段である。具体的には、コンテンツ送出手段910は、コンテンツ暗号化手段905から受け取ったTSパケット1100を、RTPパケットに設定して、ネットワーク103を通じて端末装置102に送出する。なお、TSパケット1100をRTPパケットで送出する方法としては、RFC2250 (RTP Payload Format for MPEG-1/MPEG-2 Video) に記載されているフォーマットを用いる方法などが挙げられる。

#### 【0091】

なお、ここでは、コンテンツDB903に蓄積されたコンテンツを読み出し、コンテンツ取得手段902においてリアルタイムエンコードする場合の例を示したが、予めオフラインでPES (ES) あるいはTSを生成しておき、コンテンツDB903に蓄積しておくことにより、コンテンツ取得手段902は、コンテンツ送出時に、コンテンツDB903からPESやTSを読み出す処理のみをさせるようにしても良い。

#### 【0092】

また、ここでは、コンテンツDB903に蓄積された非暗号のコンテンツを、コンテンツ暗号化手段905で送出時に暗号化する場合の例を示したが、予め暗号化されたTSを格納しておくようにすることもできる。

#### 【0093】

以上、図9～図11を用いて、配信センター101から端末装置102にコンテンツを送出するコンテンツ配信サーバ101cの構成についての詳細な説明を

終了する。

#### 【0094】

図12は、図1に示される配信センター101における利用実績収集サーバ101eの詳細な構成を示す機能ブロック図である。

利用実績収集サーバ101eは、第1の時刻情報取得手段1201と、第2の時刻情報取得手段1202と、利用実績取得手段1203と、利用実績DB1204とから構成される。

#### 【0095】

第1の時刻情報取得手段1201は、端末装置102から第1の時刻情報を取得するための手段である。具体的には、第1の時刻情報取得手段1201は、端末装置102でコンテンツの利用実績として記録した第1の時刻情報を、ネットワーク103を介して受信する。端末装置102との通信については、第1の時刻情報のセキュリティを確保するため、端末装置102との間でPKI (Public Key Infrastructure) を用いたSACを確立してから第1の時刻情報の受信を行ったり、相互認証を行わずに、利用実績収集サーバ101eと端末装置102のみが知りうる暗号鍵によって、第1の時刻情報を暗号化してから通信を行ったりすることができる。

#### 【0096】

第2の時刻情報取得手段1202は、コンテンツ配信サーバ101cから第2の時刻情報を取得するための手段である。具体的には、第2の時刻情報取得手段1202は、コンテンツ配信サーバ101cの第2の時刻情報記録手段909においてコンテンツID毎に保持されている、コンテンツの開始時の第1の時刻情報(STC)の値を、コンテンツIDと共にLAN101nを通じて取得する処理を行う。

#### 【0097】

利用実績取得手段1203は、第1の時刻情報と第2の時刻情報とから、利用実績を算出するための手段である。具体的には、利用実績取得手段1203は、第1の時刻情報取得手段1201が取得した第1の時刻情報と、第2の時刻情報取得手段1202が取得した第2の時刻情報との差分から、ユーザが当該コンテ

コンテンツのどの部分を利用したかという情報を利用実績として取得する処理を行う。  
この処理について、図13を参照して詳細に説明する。

#### 【0098】

図13は、利用実績取得手段1203が取得する第1の時刻情報と第2の時刻情報の内容を説明するための図である。図13の横軸（矢印）はコンテンツの送出に伴う時間経過を示しており、左から右に進むにつれて、時刻が進んでいくことを表している。この横軸の下に記載されているコンテンツの先頭からの相対時刻（RT）の値は、コンテンツの先頭（RT\_\_T）が0であり、時間経過にしたがって単調増加する値である。また、第1の時刻情報（PCR）の値は、コンテンツ配信サーバ101c内の計時手段907で計時されたSTCが、第1の時刻情報付加手段908によってTSパケット1100のPCR1125aに設定された値が記されている。

#### 【0099】

ここで、あるコンテンツが、PCRの値が10000（PCR\_\_T）の時点で送出を開始され（すなわち、コンテンツの先頭を示す）、PCRの値が24000（PCR\_\_E）の時点で送出を完了した（すなわち、コンテンツの末尾を示す）場合を考える。このように送出されたコンテンツを、あるユーザが、PCRの値が16000（PCR\_\_S）の時点で視聴開始し、PCRの値が20000（PCR\_\_E）の時点で視聴終了したとすると、端末装置102で記録される第1の時刻情報は、PCR\_\_SおよびPCR\_\_E、すなわち、16000および20000という値が記録されることになる。

#### 【0100】

一方、コンテンツ配信サーバ101cにおける第2の時刻情報記録手段909は、コンテンツの送出が開始された時点でのPCRの値である10000（PCR\_\_T）を第2の時刻情報として記録する。ゆえに、利用実績取得手段1203は、 $(RT\_S) = (PCR\_S - PCR\_T)$ 、および、 $(RT\_E) = (PCR\_E - PCR\_T)$ という計算式によって、コンテンツ内のどの部分を利用したか（コンテンツ内の利用開始位置および利用終了位置）という利用実績、すなわち、コンテンツの先頭からの相対時刻である、6000（RT\_\_S）およ

び10000 (RT\_\_E) という値が算出されることになる。

#### 【0101】

利用実績DB1204は、利用実績を管理するデータベース手段である。具体的には、利用実績DB1204は、利用実績取得手段1203から取得した利用実績を受け取り、図14に示す利用実績管理テーブル1400に記録する。図14に示す利用実績管理テーブル1400は、ユーザID1401、端末ID1402、コンテンツID1403、ライセンスID1404、利用実績1405とから構成されている。

#### 【0102】

ユーザID1401は、ユーザをコンテンツ利用実績収集システム1内で特定するためのIDである。

端末ID1402は、端末装置102をコンテンツ利用実績収集システム1内で特定するためのIDが記録されている。

#### 【0103】

コンテンツID1403は、端末装置102において利用されたコンテンツを、コンテンツ利用実績収集システム1内で特定するためのIDである。

ライセンスID1404は、コンテンツID1403で特定されるコンテンツの利用を許諾したライセンス(LT700)を、コンテンツ利用実績収集システム1内で特定するためのIDである。なお、ライセンスID1404は、運用に応じて、ユーザID1401や端末ID1402などに対して一意であっても良い。

#### 【0104】

利用実績1405は、利用実績収集サーバ101eの利用実績取得手段1203によって算出された利用実績を示している。

例えば、ユーザ「USER-ID-00001」は、「TERMINAL-ID-00001」なる端末装置102において、コンテンツ「CONTENT-ID-22222」を利用したことを示している。また、コンテンツ「CONTENT-ID-22222」の利用を許諾したLT700を特定するためのライセンスID1404が、「LICENSE-ID-223606」であることを

示している。利用実績 1405 は、ユーザ「USER-ID-00001」がコンテンツ「CONTENT-ID-22222」を利用したコンテンツ内の位置を特定する情報が示されており、例えば、「Play::3970584、3999999」の場合は、当該コンテンツの再生（視聴）が、コンテンツの先頭からの相対時刻として、3970584 から 3999999 の間であったことを示している。

#### 【0105】

なお、コンテンツ開始からの実時間は、PCR の単位が 27000000/1 秒であることより算出することができる。また、ユーザ「USER-ID-00002」の利用実績 1405 の利用実績では、ユーザが行った「アクション」（Play）と、アクションを行った「時刻」（2000/12/31 19:00:00）が記録されており、さらに、特殊再生を行ったコンテンツの部分特定するための情報として、Fwd（早送り）、Rwd（巻き戻し）に関する利用実績が算出されている例が示されている。

#### 【0106】

以上、図 2～図 14 を用いて、配信センター 101 における権利管理サーバ 101b、コンテンツ配信サーバ 101c、利用実績収集サーバ 101e について説明した。なお、配信センター 101 における課金サーバ 101a、ウェブサーバ 101d の詳細な構成については、本発明の主眼ではないため、ここでは省略する。

#### 【0107】

次に、コンテンツ利用実績収集システム 1 における端末装置 102 の構成について説明する。図 15 は、図 1 に示される端末装置 102 の詳細な構成を示す機能ブロック図である。

#### 【0108】

端末装置 102 は、ライセンスを処理し、セキュアにコンテンツの利用制御を行う権利管理部 1500 と、セキュアにコンテンツを利用するコンテンツ利用部 1520 と、主としてユーザに対してインタフェースを提供する端末アプリケーション 1550 とから構成されている。

**【0109】**

権利管理部1500は、第2の送受信手段1501と、ライセンス取得手段1502と、コンテンツ利用制御手段1503と、セキュアDB1504と、利用実績取得手段1505と、利用実績送信手段1506とから構成されている。また、コンテンツ利用部1520は、コンテンツ復号手段1521と、コンテンツ利用手段1522と、第1の時刻情報記録手段1523とから構成されている。

**【0110】**

第2の送受信手段1501は、ネットワーク103を通じて、配信センター101と通信するための手段である。

ライセンス取得手段1502は、権利管理サーバ101bからLT700を取得する手段である。具体的には、ライセンス取得手段1502は、図1.6に示す期待LT情報(Expected LT Information、以下ELIと記述)1600を生成し、ELI1600を権利管理サーバ101bに送信することにより、権利管理サーバ101bからLT700を取得する。

**【0111】**

図1.6において、ELI1600は、ELI識別子1601と、端末ID1602と、利用条件ID1603と、コンテンツID1604と、期待利用回数1605とから構成される。ELI識別子1601には、このデータがELI1600であることを示す情報が記述される。端末ID1602には、ELI1600を生成した端末装置102、すなわち、LT700を要求する端末装置102の端末IDが記述される。利用条件ID1603には、権利管理サーバ101bの利用条件DB203において管理されるユーザの利用条件を特定するための利用条件ID502が記述される。この利用条件ID502は、ユーザが権利管理サーバ101bから利用可能な権利を問い合わせる際のレスポンスで通知される利用条件IDを使用する。コンテンツID1604には、利用したいコンテンツのコンテンツIDが記述される。期待利用回数1605には、要求するLT700のLTアクションタグブロック702における回数カウンタ722に設定されるコンテンツの利用可能な回数の値を記述する。なお、期待利用回数1605に加え、ユーザが期待するLT700の有効期間(LTヘッダ701におけるLT

有効期間 715) を要求するようにしても良い。

【0112】

コンテンツ利用制御手段 1503 は、LT700 に基づき、セキュアにコンテンツの利用制御を行う。具体的には、コンテンツ利用制御手段 1503 は、ユーザからコンテンツの利用を要求された場合に、ライセンス取得手段 1502 が権利管理サーバ 101b より取得した LT700 に含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、暗号化コンテンツを復号するためのコンテンツ鍵をコンテンツ復号手段 1521 に渡す、という処理を行う。

【0113】

例えば、コンテンツ利用制御手段 1503 は、LT700 の LT ヘッダ 701 に設定された LT 有効期間 715 と、LT アクションタグブロック 702 に設定された回数カウンタ 722 を参照し、コンテンツが利用可能であるかどうかを判定する。端末装置 102 に保持している、図 15 には図示しないセキュアな計時手段により提供される現在時刻を参照し、現在時刻が LT 有効期間 715 内であり、かつ、回数カウンタ 722 の値が 1 以上の場合において、コンテンツの再生が可能であると判定するという処理を行う。

【0114】

なお、コンテンツ利用制御手段 1503 とコンテンツ復号手段 1521 との間は、セキュアにコンテンツ鍵を送受信するため、SAC を確立して安全にコンテンツ鍵の送受信が行われる。但し、コンテンツ利用制御手段 1503 とコンテンツ復号手段 1521 とが、同一の耐タンバ領域にある場合は、安全にコンテンツ鍵の送受信を行うことができるので、SAC を確立する必要はない。

【0115】

また、コンテンツ利用制御手段 1503 は、コンテンツの利用制御を行った結果、コンテンツの利用実績を生成する。具体的には、コンテンツ利用制御手段 1503 は、ユーザのコンテンツ利用回数（例えば再生）や、コンテンツ利用時刻といった利用実績を生成し、利用実績取得手段 1505 に渡すという処理を行う。

。

## 【0116】

セキュアDB1504は、セキュアにデータを管理するためのデータベース手段であり、ライセンス取得手段1502により取得されたLT700や、利用実績取得手段1505により取得されたコンテンツの利用実績であるUL (Usage Log、以下、ULと記述) を蓄積する。なお、ULの構成については、後で図17を用いて詳細に説明する。具体的には、セキュアDB1504は、図7で示される権利管理サーバ101bから取得したLT700や、コンテンツの利用実績であるULなどを蓄積すると共に、改ざん等の不正な行為を防止するため、セキュアDB1504中のLT700、あるいは、ULのハッシュ値を、ハード的またはソフト的に耐タンパ化された領域に格納する。

## 【0117】

利用実績取得手段1505は、コンテンツ利用制御手段1503およびコンテンツ利用手段1522からの利用実績を収集する。具体的には、利用実績取得手段1505は、コンテンツ利用制御手段1503あるいはコンテンツ利用手段1522により取得された利用実績を受け取り、セキュアDB1504に記録する。なお、即座に利用実績を配信センター101に送信するため、セキュアDB1504に記録せずに利用実績送信手段1506に送信しても良い。

## 【0118】

利用実績送信手段1506は、端末装置102で記録した利用実績を配信センター101へ送信する手段であり、記録した利用実績をULに設定して、利用実績収集サーバ101eへ送信する。具体的には、利用実績送信手段1506は、定期的または任意のタイミングでセキュアDB1504を検索し、LT700の利用実績収集指示タグブロック704内に含まれる利用実績返却条件813を参照することにより、利用実績収集サーバ101eにアップロード可能な利用実績(UL)を取得する。例えば、LT700とID等を用いて関連付けられたULを検索する方法などにより、対応するULを取得することができる。なお、このとき、LT700以外で指示された条件に基づいてULを送信したり、予め決められた条件に基づいてULを送信したりしても良い。このように取得したULを、利用実績収集サーバ101eに送信する。また、利用実績取得手段1505か

ら受け取った利用実績を、ULを用いて即座に利用実績収集サーバ101eに送信したりすることもできる。

#### 【0119】

一方、コンテンツ利用部1520は、コンテンツ復号手段1521と、コンテンツ利用手段1522と、第1の時刻情報記録手段1523とから構成されている。

#### 【0120】

コンテンツ復号手段1521は、コンテンツを復号すると共に、コンテンツ内の再生位置などの利用実績を取得する手段である。

具体的には、コンテンツ復号手段1521は、暗号化されたMPEG-2 TSにより多重化されたコンテンツを取得し、トランスポートストリームに含まれるPAT、PMTなどのPSI情報を参照して、コンテンツの映像、音声、データを含むTSパケット1100、および、PCR1125aが挿入されているTSパケット1100のPIDを取得する。

#### 【0121】

そして、コンテンツ利用制御手段1503から取得するコンテンツ鍵によって、TSP Header1110中のTransport\_Scrambling\_Control (図11に図示せず)を参照して暗号化されているTSパケット1100のペイロードを復号する。同時に、PMTに記載されているPCR\_PID (PCRが含まれているPIDを示す)を参照することにより、TSパケット1100のAdaptation\_field1120にPCR1125aが挿入されているPIDのTSパケット1100を取得して、ユーザの操作が行われた時点でのPCR1125aの値を第1の時刻情報として取得する。例えば、コンテンツの視聴(再生)開始の時点、あるいは、コンテンツの視聴終了の時点でのPCR1125aの値を第1の時刻情報として取得し、第1の時刻情報記録手段1523に送信する。また、早送り、巻き戻しについても、これらの操作の開始、終了時点でのPCR1125aの値を第1の時刻情報として取得し、第1の時刻情報記録手段1523に送信するようにすることもできる。

#### 【0122】

コンテンツ利用手段1522は、コンテンツをデコードして、図15に示さないモニターなどに出力するための手段である。具体的には、コンテンツ利用手段1522は、トランスポートストリーム中のPCR1125aを取得して、コンテンツ利用手段1522が有するPLL (Phased Lock Loop) 機能により、コンテンツ配信サーバ101cのSTC (計時手段907) と、コンテンツ利用手段1522が有するSTC (図示せず) と同期させる。そして、TSパケット1100のTSP Payload1130からPESパケット1000のデータを取得して、MPGE-2あるいはMPEG-4の映像、音声、データなどのESをデコードして、モニターに出力する。また、コンテンツの利用を終了すると、利用終了通知をコンテンツ利用制御手段1503に通知する。

#### 【0123】

第1の時刻情報記録手段1523は、コンテンツ復号手段1521において取得した第1の時刻情報を記録する。具体的には、第1の時刻情報記録手段1523は、コンテンツ復号手段1521から、コンテンツの利用開始時および利用終了時の第1の時刻情報を取得して、例えば、コンテンツ利用終了時などの適当なタイミングにおいて、利用実績取得手段1505に第1の時刻情報を送信する。

#### 【0124】

なお、端末装置102のうち、特にセキュリティを必要とするデータを処理する手段、具体的には、ライセンス取得手段1502、コンテンツ利用制御手段1503、セキュアDB1504、利用実績取得手段1505、利用実績送信手段1506、コンテンツ復号手段1521、コンテンツ利用手段1522、第1の時刻情報取得手段1523は、悪意のあるユーザによる不正な利用を防止するため、ハードウェア的に耐タンパ化されたシステムLSIや、ソフトウェア的に耐タンパ化されたプログラム等で実現されるのが一般的である。

#### 【0125】

なお、セキュアDB1504では、端末装置102をコンテンツ利用実績収集システム1内で一意に特定可能なID (端末ID) を管理しているが、権利管理部1500が端末装置102と分離可能な構成になっている場合等は、端末IDとして、権利管理部1500をコンテンツ利用実績収集システム1内で一意に特

定可能なIDを用いるようにしても良い。

#### 【0126】

以上、図15を用いて、端末装置102の詳細な構成についての説明を終了する。

ここで、利用実績取得手段1505が配信センター101に送信するためのデータ構造であるUL1700の構成について、図17を用いて詳細に説明する。

#### 【0127】

図17は、UL1700の構成の一例を示す図であり、UL1700をコンテンツ利用実績収集システム1毎、あるいは、ユーザ毎で一意に特定可能な識別子であるUL識別子1701と、UL1700全体のサイズを示すULサイズ1702と、UL1700を生成したユーザを特定するためのユーザID1703と、UL1700を生成した端末装置102を特定するための端末ID1704と、ユーザが利用したコンテンツとUL1700とを関連づけるためのコンテンツID1705と、ユーザが利用したライセンス(LT700)とUL1700とを関連づけるためのライセンスID1706と、ユーザがコンテンツを操作した内容(種類)を特定するためのアクション種別1707と、ユーザがコンテンツの操作開始した絶対時刻である利用開始時刻1708と、UL1700に設定される時刻情報1710の個数を示す時刻情報個数1709と、コンテンツ復号手段1521が取得するコンテンツの利用開始、利用終了時点での第1の時刻情報(TSパケット1100のPCR1125a)の値である時刻情報1710とから構成されている。

#### 【0128】

ここで、ライセンスID1706は、例えば、端末装置102から利用実績収集サーバ101eへのUL1700の収集時において、利用実績の返却を指示する条件が記述されたLT700のライセンスID712と一致する、ライセンスID1706を有するUL1700を検索するために使用することができる。また、UL1700からユーザが用いたLT700を特定することができるため、LT700を権利管理サーバ101bに返却するようなコンテンツ利用実績収集システムでは、配信センター101において、利用実績とユーザが所有するLT

700内に含まれる情報（例えば、LT有効期間715など）とを関連づけて管理することが可能となる。ここでは、本コンテンツの利用を許諾したLT700のライセンスID712に設定されている「LICENSE-ID-223606」が、ライセンスID1706に設定されている場合の例を示している。

#### 【0129】

また、アクション種別1707は、「再生」、「コピー」、「印刷」等の、コンテンツに対するユーザのアクションを特定するための種別であって、LT700のアクションID721の値が設定される。ここでは、コンテンツの再生を示す「Play」の例が示されている。

#### 【0130】

さらに、時刻情報1710は、ユーザがコンテンツの利用を行った部分を特定するための情報であって、コンテンツの利用開始を表す時刻情報である開始時刻情報と、コンテンツの利用終了を表す時刻情報である終了時刻情報との組が、時刻情報個数1709に設定された個数分だけ存在する。ここでは、「開始時刻情報、終了時刻情報」の組が5個あり、「開始時刻情報1、終了時刻情報1」が「13970584、13999999」、「開始時刻情報5、終了時刻情報5」が「32141683、39705843970」である場合が示されている。

#### 【0131】

なお、UL1700には、UL1700の改ざんを検出するためのハッシュ値などは存在していないが、必要に応じて改ざん検出を追加するようにしても良い。

#### 【0132】

以上、図17を用いて、端末装置102から利用実績収集サーバ101eに第1の時刻情報を含む利用実績を送信するためのデータ構造であるUL1700について、その詳細な構成について説明を行った。

#### 【0133】

さて、以上のように構成された端末装置102において、ユーザが権利管理サーバ101bからLT700を取得してセキュアにコンテンツを利用し、コンテンツ内の視聴位置を特定するための情報である、第1の時刻情報を利用実績とし

て記録し、利用実績を端末装置 102 から利用実績収集サーバ 101 e に送信する、という一連の動作を、図 18～図 24 に示すフローチャートを用いて説明する。

#### 【0134】

なお、ユーザが権利管理サーバ 101 b から LT700 を取得するにあたって、事前にウェブサーバ 101 d 等を用いたサービスプロバイダへの会員登録、コンテンツの利用条件の購入等の処理が必要であるが、これらの処理については本発明の主眼ではないため、以下の説明では省略する。

#### 【0135】

最初に、端末装置 102 において、ユーザが権利管理サーバ 101 b から LT700 を取得する動作を、図 18 に示すフローチャートを用いて説明する。

まずユーザが、端末アプリケーション 1550 が提供するユーザインタフェース手段により、権利管理サーバ 101 b で管理されているユーザの利用条件一覧を取得し、利用条件一覧から利用したいコンテンツの利用条件を選択すると、端末装置 102 は、該当する利用条件の LT700 を権利管理サーバ 101 b に要求するための ELI1600 を作成し、権利管理サーバ 101 b に送信する（ステップ S1801）。

#### 【0136】

具体的には、コンテンツ利用手段 1522 は、ユーザが選択した利用条件が利用を許諾するコンテンツのコンテンツ ID を端末アプリケーション 1550 から受け取り、コンテンツ利用制御手段 1503 に送信する。コンテンツ利用制御手段 1503 はコンテンツ ID をライセンス取得手段 1502 に送信し、ライセンス取得手段 1502 はコンテンツ利用制御手段 1503 から受信したコンテンツ ID を基に、図 16 に示した ELI1600 を生成する。

#### 【0137】

なお、この ELI1600 に設定する利用条件 ID 1603 は、端末アプリケーション 1550 または権利管理部 1500 が権利管理サーバ 101 b やウェブサーバ 101 d 経由でユーザが所有する利用条件を予め問い合わせることにより、利用条件 ID 1603 を取得済みであるものとする。また、期待利用回数 16

05については、端末アプリケーション1550を通じて、ユーザが希望する値を設定するようにしても良いし、予めサービスの運用などにより決められた値を設定するようにしても良い。このようにして生成されたELI1600は、第2の送受信手段1501を通じて、権利管理サーバ101bに送信される。

#### 【0138】

権利管理サーバ101bのライセンス発行手段212は、端末装置102からELI1600を受信すると、ユーザ情報DB201を参照し、ユーザを特定することにより、ユーザ認証を行う（ステップS1802）。

#### 【0139】

具体的には、ユーザ認証は2段階で行なわれる。通常、LT700のようなセキュリティを要するデータのやり取りを行う際には、SACを確立して安全に通信を行えるようにするのが一般的である。よって、第1段階としては、権利管理サーバ101bと端末装置102との間でSACを確立する。SACの確立には、例えばSSLやTLS（Transport Layer Security）を利用することができる。この相互認証によって、権利管理サーバ101bは、端末装置102が正しい端末ID1602を有することが確認できる。

#### 【0140】

第2段階として、ライセンス発行手段212が端末ID1602なる端末装置102を所有するユーザを特定する。そこでライセンス発行手段212は、ELI1600に含まれる端末ID1602を取得し、ユーザ情報DB201のユーザ情報管理テーブル300のユーザID301および端末ID302を参照して、ELI1600に含まれる端末ID1602と一致するユーザ情報管理テーブル300の端末ID302を検索する。一致する端末ID302が見つかった場合には、関連するユーザID301を取得することができるが、一致する端末ID302が見つからなかった場合には、ユーザ認証は失敗する。

#### 【0141】

ライセンス発行手段212は、ステップS1802のユーザ認証結果を確認する（ステップ1803）。

ステップS1803において、YESである場合、すなわち、正しくユーザ認

証が行なわれた場合には、LT700を発行するための利用条件の確認を行うため、ステップS1804を実行する。

#### 【0142】

ステップS1803において、NOである場合、すなわち、正しくユーザ認証が行なわれなかった場合には、LT発行不可と判定され、ライセンス発行手段212はLT発行不可通知を端末装置102に送信する。

#### 【0143】

ライセンス発行手段212は、LT発行可否判定処理を実行する（ステップS1804）。このLT発行可否判定処理については、後で図19を用いて詳細に説明する。

#### 【0144】

ライセンス発行手段212は、LT発行可否判定処理の結果を参照し、LT700が発行可能か否かを判定する（ステップS1805）。

ステップS1805において、YESである場合、すなわち、LT発行可能と判定された場合には、ステップS1806を実行する。

#### 【0145】

ステップS1805において、NOである場合、すなわち、LT発行不可と判定された場合には、ライセンス発行手段212はLT発行不可通知を端末装置102に送信する。

#### 【0146】

ライセンス発行手段212は、利用実績収集指示手段211に対して、図8に示した利用実績の収集のための指示情報803を生成するように要求し、利用実績収集指示手段211において、利用実績収集指示生成処理が実行される（ステップS1806）。この利用実績収集指示生成処理については、後で図を用いて詳細に説明する。

#### 【0147】

ライセンス発行手段212は、利用実績収集指示手段211から利用実績の収集のための指示情報803を受信し、LT700を生成する（ステップS1807）。

## 【0148】

具体的には、ライセンス発行手段212は、利用実績収集指示手段211から指示情報803を受信し、利用実績収集指示タグブロック704を生成する。また、ELI1600および利用条件DB203の利用条件管理テーブル500を参照すると共に、コンテンツ鍵DB202のコンテンツ鍵管理テーブル400から、コンテンツID1604（コンテンツID401）に対応するコンテンツ鍵402を取得し、ELI1600により要求された利用条件を含むLT700を生成する。

## 【0149】

ライセンス発行手段212は、利用条件DB203の利用条件管理テーブル500を更新する（ステップS1808）。具体的には、ライセンス発行手段212は、発行したLT700に含まれる利用条件の分だけ、当該ユーザの利用条件を減算する処理を行う。例えば、利用条件管理テーブル500の利用可能回数505が「5」である場合に、LT700のLTアクションタグブロック702の回数カウンタ722が「3」であった場合には、利用条件管理テーブル500の利用可能回数505を「2」に更新するという処理を行う。

## 【0150】

ライセンス発行手段212は、ステップS1807において生成したLT700を端末装置102に送信する（ステップS1809）。具体的には、ライセンス発行手段212は、第1の送受信手段213を通じて、端末装置102にLT700を送信する処理を行う。

## 【0151】

端末装置102のライセンス取得手段1502は、権利管理サーバ101bからLT700を受信し、LT700をセキュアDB1504に登録する（ステップS1810）。具体的には、ライセンス取得手段1502は、第2の送受信手段1501を通じて、ステップS1801で生成したELI1600に対するレスポンスとしてLT700を取得し、LT700をセキュアDB1504に書き込み、セキュアDB1504のハッシュ値を更新する。

## 【0152】

なお、ステップS1803またはステップS1805において、LT700が発行不可であるためにLT発行不可通知が送信された場合、端末装置102のライセンス取得手段1502は、LT発行不可通知を受信する（ステップS1811）。具体的には、端末装置102のライセンス取得手段1502は、権利管理サーバ101bからのLT発行不可通知を受信し、端末アプリケーション1550のユーザインタフェース手段を通じて、ユーザにその旨を通知して、本処理を終了する。

#### 【0153】

ここで、ステップS1804のLT発行可否判定処理について、図19を用いて説明する。

まず、ライセンス発行手段212は、ELI1600で指定された利用条件ID1603が利用条件DB203の利用条件管理テーブル500に存在するかどうかを確認する（ステップS1901）。具体的には、ライセンス発行手段212は、端末装置102から受信したELI1600を参照し、利用条件ID1603を取得する。この利用条件ID1603が、利用条件管理テーブル500中の利用条件ID502と一致するものがあるかどうかを確認する。

#### 【0154】

ステップS1901において、YESである場合、すなわち、利用条件管理テーブル500にELI1600の利用条件ID1603と一致する利用条件ID502が存在する場合には、さらに、利用条件ID502を有するユーザID501が、図18におけるステップS1802で認証に成功した、ユーザ情報DB201のユーザ情報管理テーブル300中のユーザID301と一致するかどうかを確認する。ここで当該ユーザIDが一致した場合には、ステップS1902を実行し、当該ユーザIDが一致しない場合には、ステップS1905を実行する。

#### 【0155】

ステップS1901において、NOである場合、すなわち、利用条件管理テーブル500にELI1600の利用条件ID1603と一致する利用条件ID502が存在しない場合には、ステップS1905を実行する。

## 【0156】

次に、ライセンス発行手段212は、ユーザの利用条件が、有効期限を満たしているかどうかを判定する（ステップS1902）。具体的には、ライセンス発行手段212は、利用条件DB203の利用条件管理テーブル500中の有効期間504を参照するとともに、セキュアな計時手段（図2に図示せず）から現在時刻を取得し、現在時刻が有効期間504で示される開始日時から終了日時の間に含まれているか否かを判定する。

## 【0157】

例えば、利用条件管理テーブル500中の有効期間504が「2002/12/20 12:12:12」である場合に、現在時刻が「2002/12/18 12:34:56」であれば、ユーザの利用条件が有効期限内であると判定される。一方、現在時刻が「2002/12/31 19:00:00」であれば、ユーザの利用条件は有効期限外であると判定される。

## 【0158】

ステップS1902において、YESである場合、すなわち、ユーザの利用条件が有効期限内である場合には、ステップS1903を実行する。

ステップS1902において、NOである場合、すなわち、ユーザの利用条件が有効期限外である場合には、ステップS1905を実行する。

## 【0159】

ライセンス発行手段212は、ELI1600の期待利用回数1605が、ユーザの所有する利用条件内であるか否かを判定する（ステップS1903）。具体的には、ライセンス発行手段212は、ELI1600で指定された期待利用回数1605が、利用条件管理テーブル500の利用可能回数505以内であるかどうかを確認する。例えば、利用条件管理テーブル500の利用可能回数505が「5」である場合に、ELI1600で指定された期待利用回数1605が「3」であれば、ELI1600で指定された期待利用回数1605はユーザの利用条件に含まれると判定される。一方、ELI1600で指定された期待利用回数1605が「10」であれば、ELI1600で指定された期待利用回数1605はユーザの利用条件には含まれないと判定される。

**【0160】**

ステップS1903において、YESである場合、すなわち、期待利用回数1605がユーザの利用条件に含まれる場合には、ステップS1904を実行する。

**【0161】**

ステップS1903において、NOである場合、すなわち、期待利用回数1605がユーザの利用条件に含まれない場合には、ステップS1905を実行する。

**【0162】**

ライセンス発行手段212は、LT700が発行可能と判定して、LT発行可否判定処理を終了する（ステップS1904）。

また、ステップS1901～ステップS1903において、NOである場合、すなわち、ライセンス発行手段212がLT700を発行不可能と判定した場合には、LT発行可否判定処理を終了する（ステップS1905）。

**【0163】**

以上、図19を用いて、LT発行可否判定処理の説明を行った。

また、ステップS1806の利用実績収集指示生成処理について、図20を用いて説明する。

**【0164】**

利用実績収集指示手段211は、利用実績収集条件DB204から、ELI1600で指定されたコンテンツID1604に対応する利用実績収集条件602等を取得する（ステップS2001）。具体的には、利用実績収集指示手段211は、利用実績収集条件DB204の利用実績収集条件管理テーブル600を参照し、ELI1600で指定されたコンテンツID1604と、コンテンツID601が一致する利用実績収集条件602を取得する。

**【0165】**

次に、利用実績収集指示手段211は、ステップS2001で取得した利用実績収集条件602の対象ユーザ決定条件603が、ユーザのプライバシーポリシーを考慮する必要があるか否かを判定する（ステップS2002）。具体的には、

利用実績収集指示手段 211 は、対象ユーザ決定条件 603 を参照し、当該コンテンツに関する利用実績の収集について、ユーザが設定したプライバシーポリシーを考慮する必要があるか否かを判断する。例えば、図 6 のコンテンツ ID 601 が「CONTENT-ID-00003」の対象ユーザ決定条件 603 は、プライバシーポリシーを考慮するよう設定されている例が示されている。

#### 【0166】

ステップ S2002 において、YES である場合、すなわち、ユーザのプライバシーポリシーを考慮する必要がある場合には、ステップ S2003 を実行する。

ステップ S2002 において、NO である場合、すなわち、ユーザのプライバシーポリシーを考慮する必要がある場合には、ステップ S2005 を実行する。

#### 【0167】

利用実績収集指示手段 211 は、ユーザ情報 DB 201 を参照し、ユーザのプライバシーポリシーを取得する（ステップ S2003）。具体的には、利用実績収集指示手段 211 は、ユーザ情報 DB 201 のユーザ情報管理テーブル 300 のプライバシーポリシー 304 を取得する。

#### 【0168】

利用実績収集指示手段 211 は、ステップ S2003 で取得したプライバシーポリシー 304 を参照し、当該ユーザが利用実績の収集を許可しているか否かを判定する（ステップ S2004）。具体的には、利用実績収集指示手段 211 は、プライバシーポリシー 304 が「実績収集 OK」である場合には、利用実績の収集が認められていると判定する。一方、プライバシーポリシー 304 が「実績収集 NG」である場合には、利用実績の収集が拒否されていると判定する。

#### 【0169】

ステップ S2004 において、YES である場合、すなわち、利用実績の収集が OK である場合には、ステップ S2005 を実行する。

ステップ S2004 において、NO である場合、すなわち、利用実績の収集が NG である場合には、利用実績記録条件 811 の生成は不要となるため、本処理を終了する。

#### 【0170】

利用実績収集指示手段 211 は、さらに、利用実績の収集を行うユーザを決定するため、権利管理サーバ 101b の各種データベースを参照する必要があるか否かを判定する（ステップ S2005）。具体的には、利用実績収集指示手段 211 は、ステップ S2001 で取得した対象ユーザ決定条件 603 を参照して、利用条件 DB 203 等を参照する必要があるか否かを判定する。例えば、図 6 のコンテンツ ID 601 が「CONTENT-ID-00004」なるコンテンツの対象ユーザ決定条件 603 は、「UR10 権利以上」となっており、利用条件 DB 203 に該当ユーザの利用条件が 10 以上存在する場合にのみ、利用実績の収集を行う対象ユーザと決定されるようになっているため、利用条件 DB 203 へのアクセスが発生する。

#### 【0171】

ステップ S2005 において、YES である場合、すなわち、利用実績の収集の対象ユーザを決定するために、データベースへのアクセスが発生する場合には、ステップ S2006 を実行する。

#### 【0172】

ステップ S2005 において、NO である場合、すなわち、利用実績の収集の対象ユーザを決定するために、データベースへのアクセスが発生しない場合には、ステップ S2009 を実行する。

#### 【0173】

利用実績収集指示手段 211 は、対象ユーザ決定条件 603 に記載された条件に応じたデータベースを参照し、当該ユーザに関するデータを取得する（ステップ S2006）。

#### 【0174】

利用実績収集指示手段 211 は、データベースから取得した情報を基に、利用実績の収集の対象ユーザとなるか否かを決定する（ステップ S2007）。具体的には、利用実績収集指示手段 211 は、ステップ S2006 で取得した当該ユーザに関するデータを参照し、対象ユーザ決定条件 603 を満たすか否かを判定する。例えば、図 6 のコンテンツ ID 601 が「CONTENT-ID-00004」なるコンテンツの場合、ステップ S2006 で利用条件 DB 203 の利用

条件管理テーブル 500 から取得した当該ユーザの利用条件の合計数が「12 件」である場合には、利用実績の収集を行う対象ユーザと決定される。

#### 【0175】

一方、ステップ S2006 で利用条件 DB 203 の利用条件管理テーブル 500 から取得した当該ユーザの利用条件の合計数が「3 件」である場合には、利用実績収集条件管理テーブル 600 の対象ユーザ決定条件 603 を満たさないため、利用実績の収集を行う対象ユーザとは決定されない。なお、ここでは、ユーザが所有する利用条件の合計数によって利用実績の収集の対象ユーザとなるか否かを決定する場合の例を示したが、利用実績収集サーバ 101e の利用実績 DB 1204 で管理されている利用実績を用い、該当ユーザの利用実績の数などによって利用実績の収集の対象ユーザとなるか否かを決定するようにすることも可能である。

#### 【0176】

利用実績収集指示手段 211 は、利用実績収集指示タグブロック 704 を生成する（ステップ S2008）。具体的には、利用実績収集指示手段 211 は、利用実績収集条件管理テーブル 600 に基づき、図 7 および図 8 に示す利用実績収集指示タグブロック 704 を生成する処理を行う。

#### 【0177】

また、ステップ S2006 において、NO である場合には、利用実績収集指示手段 211 は、対象ユーザ決定条件 603 を参照して、利用実績の収集の対象となるユーザをランダムに選択するか否かを判定する（ステップ S2009）。

#### 【0178】

ステップ S2009 において、YES である場合、すなわち、利用実績の収集の対象ユーザをランダムに選択する場合には、ステップ S2010 を実行する。

ステップ S2009 において、NO である場合、すなわち、全てのユーザから利用実績の収集を行うと判断された場合には、利用実績収集指示タグブロック 704 を生成するため、ステップ S2008 を実行する。

#### 【0179】

利用実績収集指示手段 211 は、一様乱数等による試行を行うことにより、利

用実績の収集の対象ユーザを選択するためのデータを生成する（ステップS2010）。その後、ステップS2007を実行する。

#### 【0180】

以上、ステップS1806の利用実績収集指示生成処理について説明したことにより、端末装置102が権利管理サーバ101bからLT700を取得する動作についての説明を終了する。

#### 【0181】

次に、端末装置102において、ユーザがコンテンツを利用すると共に、利用実績を記録する動作を、図21に示すフローチャートを用いて説明する。

まずユーザは、端末アプリケーション1550のブラウザを通じて、ウェブサーバ101d等が提供するウェブ画面のストリーミングコンテンツ一覧から、利用したいコンテンツを選択する。端末装置102におけるコンテンツ利用部1520は、端末アプリケーション1550から受信した該当コンテンツのコンテンツIDを権利管理部1500に送信する（ステップS2101）。具体的には、コンテンツ利用部1520のコンテンツ利用手段1522は、ユーザが選択したコンテンツIDおよびコンテンツの位置を示すURI（Unified Resource Identifier）を端末アプリケーション1550から受け取り、当該コンテンツIDを権利管理部1500のコンテンツ利用制御手段1503に送信し、該当コンテンツの利用を要求する。なお、コンテンツの利用は、本発明における実施の形態1ではコンテンツの再生を示すものとして、以下の説明を行う。

#### 【0182】

コンテンツ利用制御手段1503は、セキュアDB1504から、該当コンテンツIDに対応するLT700を取得する（ステップS2102）。具体的には、コンテンツ利用制御手段1503は、コンテンツ利用手段1522から受信したコンテンツIDをキーとしてセキュアDB1504を検索する。

#### 【0183】

コンテンツ利用制御手段1503は、ステップS2102において検索したLT700を取得し、利用可能なLT700であるか否かを判定する（ステップS

2103)。具体的には、コンテンツ利用制御手段1503は、まず、コンテンツ利用手段1522から指定されたコンテンツIDに対応するLT700が、セキュアDB1504に存在するかどうかを確認する。該当LT700が存在する場合には、LT700のLT有効期間715や回数カウンタ722を参照し、LT700の有効性を確認する。なお、LT有効期間715の有効性の確認については、端末装置102内のセキュアな計時手段（図15に図示せず）から取得した時刻情報を用いて確認するものとする。また、LT700の回数カウンタ722については、その値が「1」以上（無限回も含む）であることを確認する。なお、コンテンツ利用手段1522から指定されたコンテンツIDに対応するLT700が、セキュアDB1504に存在しない場合は、ステップS2113を実行する。

#### 【0184】

ステップS2103において、YESである場合、すなわち、LT700が利用可能であると判定された場合には、ステップS2104を実行する。

ステップS2103において、NOである場合、すなわち、LT700が利用不可能であると判定された場合には、ステップS2113を実行する。

#### 【0185】

コンテンツ利用制御手段1503は、当該コンテンツの利用に際して、利用実績を記録するか否かを判定する（ステップS2104）。具体的には、コンテンツ利用制御手段1503は、セキュアDB1504から取得したLT700の利用実績収集指示タグブロック704の有無を検出し、利用実績を記録する処理を行うか否かを決定する。なお、LT700の利用実績収集指示タグブロック704の有無により利用実績を記録するかどうかを決定する方法以外にも、利用実績収集指示タグブロック704の内容を参照したり、コンテンツ利用制御手段1503が把握可能なその他の利用実績収集指示に関わる情報を参照したりすることにより、利用実績を記録するかどうかを決定するようにしても良い。

#### 【0186】

ステップS2104において、YESである場合、すなわち、利用実績を記録すると判定された場合には、ステップS2105を実行する。

ステップS2104において、NOである場合、すなわち、利用実績を記録しないと判定された場合には、ステップS2106を実行する。

#### 【0187】

コンテンツ利用制御手段1503は、利用実績を記録する（ステップS2105）。具体的には、コンテンツ利用制御手段1503は、利用実績収集指示タグブロック704の指示情報803中の、利用実績記録条件811を参照し、その指示内容に応じた利用実績を記録する。例えば、図8に示すように、利用実績内容812として「アクション」および「時刻」が存在する場合は、セキュアな計時手段（図15に図示せず）から取得した日時情報を記録すると共に、ユーザが指示したアクションとして「Play（再生）」を記録する。このように記録した利用実績は、利用実績取得手段1505に送信される。

#### 【0188】

コンテンツ利用制御手段1503は、コンテンツ鍵を取得し、コンテンツ復号手段1521に送信する（ステップS2106）。具体的には、コンテンツ利用制御手段1503は、LT700のコンテンツ鍵タグブロック703からコンテンツ鍵を取得し、必要に応じてSACを確立して、コンテンツ復号手段1521に送信する。コンテンツ鍵の送信と同時に、コンテンツ利用制御手段1503は、LT700の利用実績収集指示タグブロック704に含まれる指示情報803の内、利用実績記録条件811および利用実績内容812の「利用部分」をコンテンツ復号手段1521に通知することにより、コンテンツ利用手段1522での利用実績の収集を指示する。

#### 【0189】

なお、このとき、コンテンツ利用制御手段1503からコンテンツ復号手段1521に対して、LT700をそのまま送信するようにしても良い。

コンテンツ復号手段1521は、コンテンツ鍵を受信する（ステップS2107）。具体的には、コンテンツ復号手段1521は、コンテンツ利用制御手段1503からコンテンツ鍵を受信すると共に、端末アプリケーション1550から取得したコンテンツのURIで指定される暗号化コンテンツを取得する。

#### 【0190】

コンテンツ復号手段1521、および、コンテンツ利用手段1522は、コンテンツの復号処理、および、利用処理（再生処理）を行うと共に、コンテンツの詳細な利用実績を取得する（ステップS2108）。具体的には、コンテンツ復号手段1521は、コンテンツ利用制御手段1503から受信したコンテンツ鍵により暗号化されたTSパケット1100を復号すると共に、TSパケット1100のPCR1125aを用いて、少なくともコンテンツの利用開始および利用終了時点での利用実績を取得する。

#### 【0191】

また、コンテンツ利用手段1522は、コンテンツ復号手段1521で復号されたTSパケット1100からPESパケット1000を取得し、PESパケット1000からコンテンツのESを取得し、デコードして、図15には示さないモニター等にコンテンツを出力する。このコンテンツ利用処理については、後で図22および図23を用いて詳細に説明する。

#### 【0192】

コンテンツ復号手段1521は、コンテンツ利用にあたって取得した利用実績を利用実績取得手段1505に送信する（ステップS2109）。

利用実績取得手段1505は、コンテンツ復号手段1521から利用実績を受信する（ステップS2110）。

#### 【0193】

利用実績取得手段1505は、コンテンツ利用制御手段1503およびコンテンツ復号手段1521において記録された有効な利用実績を取得したかどうかを判定する（ステップS2111）。具体的には、ステップS2104およびステップS2108において、利用実績収集指示タグブロック704の指示情報803の内容、あるいは、指示情報803の有無によっては、利用実績が記録されていない可能性もあるため、利用実績をセキュアDB1504に蓄積するか否かを判定するための処理である。

#### 【0194】

ステップS2111において、YESである場合、すなわち、有効な利用実績が記録されている場合には、ステップS2112を実行する。

ステップ S 2 1 1 1 において、NO である場合、すなわち、有効な利用実績が記録されていない場合には、本処理を終了する。

#### 【0195】

利用実績取得手段 1 5 0 5 は、利用実績をセキュア DB 1 5 0 4 に蓄積する（ステップ S 2 1 1 2）。具体的には、利用実績取得手段 1 5 0 5 は、図 1 7 に示すように、利用実績データ 1 8 0 3 を設定した、利用実績を記述するための UL 1 7 0 0 をセキュア DB 1 5 0 4 に書き込み、セキュア DB 1 5 0 4 の更新処理を行う。このとき、UL 1 7 0 0 のコンテンツ ID 1 7 0 5、ライセンス ID 1 7 0 6 は、それぞれ、LT 7 0 0 のコンテンツ ID 7 1 4、ライセンス ID 7 1 2 の値を用いる。

#### 【0196】

なお、ステップ S 2 1 0 3 において、利用可能な LT 7 0 0 が存在しない場合には、コンテンツ利用手段 1 5 2 2 は、コンテンツ利用制御手段 1 5 0 3 から利用不可通知を受信する（ステップ S 2 1 1 3）。コンテンツ利用手段 1 5 2 2 は、端末アプリケーション 1 5 5 0 が提供するユーザインタフェース手段を通じて、ユーザにその旨を通知する。

#### 【0197】

また、図 2 1 におけるステップ S 2 1 1 0 において、コンテンツ利用手段 1 5 2 2 からのコンテンツ利用終了通知あるいは、その他の何らかの通知が発生した場合に、コンテンツ利用制御手段 1 5 0 3 において利用実績を記録し、利用実績取得手段 1 5 0 5 に対して利用実績を送信するようにすることもできる。例えば、このタイミングでは「コンテンツの利用終了」に関する利用実績（時刻情報を含んでも良い）を取得することが可能である。

#### 【0198】

ここで、ステップ S 2 1 0 8 のコンテンツ利用処理および利用実績記録処理について、図 2 2 および図 2 3 を用いて説明する。

最初に、端末装置 1 0 2 におけるコンテンツ利用処理および利用実績記録処理について、図 2 2 を用いて説明する。

#### 【0199】

コンテンツ利用手段1522は、コンテンツ配信サーバ101cに対して、コンテンツ取得要求を送信する（ステップS2201）。具体的には、コンテンツ利用手段1522は、端末アプリケーション1550から受信したコンテンツのURIを基にコンテンツ配信サーバ101cに接続し、RTSPを用いて再生要求（PLAY）を送信する。コンテンツ配信サーバ101cは、対応するコンテンツをRTPのペイロードに設定して端末装置102に対して順次送信する。

#### 【0200】

第2の送受信手段1501は、コンテンツ配信サーバ101cからコンテンツを受信する（ステップS2202）。具体的には、第2の送受信手段1501は、コンテンツ配信サーバ101cが送信したRTPパケットを順次受信し、RTPペイロードから順次TSパケット1100を取り出し、コンテンツ復号手段1521に対して送信する。

#### 【0201】

第2の送受信手段1501は、コンテンツ配信サーバ101cからのコンテンツ受信が完了したか否かを判定する（ステップS2203）。具体的には、第2の送受信手段1501は、受信したRTPパケットが最終パケットであるか等の方法により、ストリームの終端を検出する。

#### 【0202】

ステップS2203において、NOである場合、すなわち、コンテンツの受信が完了していない場合には、ステップS2204を実行する。

ステップS2203において、YESである場合、すなわち、ユーザから端末アプリケーション1550を通じて、コンテンツ利用終了の通知を受けた場合や、コンテンツの受信が完了した場合には、端末アプリケーション1550を通じてその旨をユーザに通知し、本処理を終了する。

#### 【0203】

コンテンツ復号手段1521は、TSパケット1100を復号する（ステップS2204）。具体的には、コンテンツ復号手段1521は、第2の送受信手段1501から受信したTSパケット1100の内、ペイロード部（TSPPayload1130）が暗号化されているTSパケット1100の復号を行う。

ここで、TS パケット 1100 が暗号化されているか否かについては、TSP Header 1110 中の `transport_scrambling_control` を参照することによって判別することができる。

#### 【0204】

コンテンツ復号手段 1521 は、TS パケット 1100 の復号後、TS パケット 1100 に付加されたハッシュを用いて改ざんチェックの判定を行う（ステップ S2205）。具体的には、コンテンツ復号手段 1521 は、TS パケット 1100 を復号した後、コンテンツ配信サーバ 101c で行ったハッシュ値の計算と同様の方法により、ハッシュ値の改ざん検出を行う。すなわち、PCR 1125a と TSP Payload 1130 とのハッシュを計算して、TS パケット 1100 の Private Data 1125e に設定されたハッシュ値と一致するか否かを判定する。なお、本処理は、Adaptation Field 1120 が存在し、PCR 1125a が設定されている TS パケット 1100 についてのみ行えば良い。

#### 【0205】

ステップ S2205 において、YES である場合、すなわち、ハッシュ値が正しい場合は、ステップ S2206 を実行する。

ステップ S2205 において、NO である場合、すなわち、ハッシュ値が正しくない場合は、コンテンツの復号処理およびコンテンツの再生処理を終了して、その旨を端末アプリケーション 1550 に通知する。なお、ここで、ハッシュ値が正しくない場合、利用実績をログとして記録した上で、そのままコンテンツの復号処理およびコンテンツの再生処理を継続しても良いし、利用実績をログとして記録した上で、コンテンツの復号処理およびコンテンツの再生処理を終了（コンテンツの利用を不許可に）しても良い。あるいは、利用実績として記録しない、すなわち、ハッシュ値が正しくない部分は、利用実績から除外するようにして、コンテンツの利用を継続しても良いし、コンテンツの利用を終了するようにしても良い。

#### 【0206】

コンテンツ復号手段 1521 は、利用実績記録処理を行う（ステップ S220

6)。この利用実績記録処理については、後で図を用いて詳細に説明する。ステップS2206の処理を終了後、ステップS2202を実行する。

#### 【0207】

なお、コンテンツ利用手段1522は、コンテンツ復号手段1521から復号されたTSパケット1100を受信し、TSパケット1100のペイロード部（TSPPayload1130）から復号されたPESパケット1000を取得し、コンテンツの映像ES、音声ES等のデータを取得して、それぞれのESをデコードして、映像、音声の同期をとりつつ、図15に示さないモニター等に出力する。このとき、コンテンツ利用手段1522は、TSパケット1100のAdaptationField1120のPCR1125aを取得し、コンテンツ利用手段1522の内部に有するSTCを、PLL（図15に図示せず）を用いることにより、安定したクロックに保つ処理を行う。よって、このSTCの値と、PESパケット1000のPTS1043a、DTS1043bが一致したときにPESパケット1000のPESPacketDataBytes1060の映像ES、音声ESなどのデコード、表示を行うことにより、正常なコンテンツ再生を実現する。

#### 【0208】

なお、ステップS2205において、TSパケット1100のすり替え等を防止するため、PCR1125aが付加されている全てのTSパケット1100の改ざんチェックを行うようにしたが、例えば、利用実績としてPCR1125aを記録するTSパケット1100のみ等、必要に応じて改ざんチェックを行うようにしても良い。

#### 【0209】

次に、図22におけるステップS2206に示した、コンテンツ復号手段1521の利用実績記録処理について、図23を用いて説明する。

コンテンツ復号手段1521は、コンテンツ利用終了か否かを判定する（ステップS2301）。具体的には、コンテンツ復号手段1521は、コンテンツ利用手段1522（またはコンテンツ利用制御手段1503でも良い）からのコンテンツ利用終了通知を受信したかどうかを確認する。

**【0210】**

ステップS2301において、YESである場合、すなわち、コンテンツ利用終了である場合には、ステップS2307を実行する。

ステップS2301において、NOである場合、すなわち、コンテンツ利用終了でない場合には、ステップS2302を実行する。

**【0211】**

コンテンツ復号手段1521は、TSパケット1100が、最初のTSパケットの入力であるか否かを判定する（ステップS2302）。具体的には、コンテンツ復号手段1521は、ユーザが、再生、停止、早送り、巻戻しなどのコンテンツの利用操作（アクション）を行った後の、最初のTSパケット1100の入力であるか否かを判定する。これにより、コンテンツ復号手段1521は、利用実績であるUL1700の時刻情報に設定される開始時刻情報の値を取得することができる。

**【0212】**

ステップS2302において、YESである場合、すなわち、処理中のTSパケット1100が、ユーザ操作後の最初のTSパケット1100である場合には、ステップS2303を実行する。

**【0213】**

ステップS2302において、NOである場合、すなわち、処理中のTSパケット1100が、ユーザ操作後の最初のTSパケット1100でない場合には、ステップS2304を実行する。

**【0214】**

コンテンツ復号手段1521は、処理中のTSパケット1100のPCR1125aの値を、開始時刻情報として内部に保持する（ステップS2303）。

コンテンツ復号手段1521は、処理中のTSパケット1100のPCR1125aの値を一時記録すると共に、PCR1125aの値の変化率を算出する（ステップS2304）。具体的には、コンテンツ復号手段1521は、コンテンツ利用終了時のPCR1125aの値を得られるようにするため、処理を行った最新のTSパケット1100のPCR1125aの値を内部に保持する。また、

この一時的に記録したPCR1125aの値を用いて、以前のPCR1125aの値と処理中のTSパケット1100のPCR1125aの値の変化率を計算する。

#### 【0215】

コンテンツ復号手段1521は、PCR1125aの値の変化率が一定であるかどうかを判定する（ステップS2305）。具体的には、コンテンツ復号手段1521は、ステップS2304で算出したPCR1125aの値の変化率を監視し、変化率が「0」であるか、あるいは、変化率が「0」以外であるかをチェックする。つまり、変化率が「0」であれば、TSパケット1100がコンテンツ復号手段1521に対して一定のレートで入力されていることになるので、通常再生中であれば通常再生が継続されていることが認識可能であるし、早送り中であれば早送りが継続されていることが認識可能である。

#### 【0216】

一方、変化率が「0」を除く正の値、または、負の値であれば、入力されるTSパケット1100のレートが変化していることになるので、通常再生中から早送りに状態が変化したことや、早送り中から通常再生状態に変化したことが認識可能である。なお、TSパケット1100のロスや、PCRジッタが発生する場合も考えられるので、ある程度の範囲のPCR1125aの値を保持しておき、平均化して判定処理を行うようにしても良い。

#### 【0217】

ステップS2305において、YESである場合、すなわち、PCR1125aの変化率が0である場合には、ステップS2302を実行する。

ステップS2305において、NOである場合、すなわち、PCR1125aの変化率が0以外である場合には、ステップS2306を実行する。

#### 【0218】

コンテンツ復号手段1521は、ステップS2304において一時記録したPCR1125aの値を取得し、開始時刻情報または終了時刻情報として記録する（ステップS2306）。具体的には、コンテンツ復号手段1521内で保持している、処理済みのTSパケット1100の内、最も新しいTSパケット110

0のPCR1125aを取得して、利用実績であるUL1700の時刻情報に設定される開始時刻情報または終了時刻情報の値を取得する。

#### 【0219】

取得したPCR1125aの値が、開始時刻情報であるか、終了時刻情報であるかの判定については、コンテンツ復号手段1521が再生中であるか、早送り中であるか、巻戻し中であるか、といった処理ステータスを内部で管理することにより、PCR1125aの値の変化率の正負に応じて開始時刻情報であるか、終了時刻情報であるかを判定することができる。例えば、再生中である場合において、PCR1125aの値の変化率が正であれば、早送りが行われたことになるので、再生(Play)の終了時刻情報として記録すると共に、早送り(Fwd)の開始時刻情報として記録する。また、このとき、LT700により指定される利用実績記録条件811において、「特殊再生除外」である場合には、早送り(Fwd)の開始時刻情報として記録する処理は行う必要はない。

#### 【0220】

コンテンツ復号手段1521は、一時記録しているPCR1125aの値を、終了時刻情報として記録する(ステップS2307)。具体的には、コンテンツ復号手段1521は、コンテンツ利用終了が通知された場合、ステップS2304において内部で一時的に保持しているPCR1125aの値を、利用実績であるUL1700の時刻情報に設定される終了時刻情報として記録する。

#### 【0221】

なお、ステップS2304において、内部で一時的に保持しているPCR1125aの値を用いて、継続的にPCR1125aの変化を監視するようにしても良い。例えば、PCR1125aの値の間隔を監視し、本来単調増加であるはずのPCR1125aの値が減少した場合には、TSパケット1100の不正な差し替え(すり替え)が行われたことが検出できるので、利用実績の記録を無効化(記録しないように)したり、改ざんされた旨の利用実績(ログ)を記録したり、コンテンツ復号処理を中止したりすることができる。

#### 【0222】

以上、図23を用いて、コンテンツ復号手段1521においてコンテンツの利

用開始時刻および終了時刻を記録する処理について説明した。

次に、端末装置 102 のコンテンツ利用時における、コンテンツ配信サーバ 101c のコンテンツ送信処理について、図 24 を用いて説明する。

#### 【0223】

コンテンツ配信サーバ 101c におけるコンテンツ取得要求受信手段 901 は、端末装置 102 からのコンテンツ取得要求を受信する（ステップ S2401）。具体的には、コンテンツ取得要求受信手段 901 は、端末装置 102 から RTP によって再生要求を受け、要求されたコンテンツ ID を取得して、コンテンツ ID をコンテンツ取得手段 902 に送信する。

#### 【0224】

コンテンツ送出手段 910 は、コンテンツの送出が完了したか否かを判定する（ステップ S2402）。具体的には、コンテンツ送出手段 910 は、コンテンツの全てを RTP パケットとして端末装置 102 に送出したか否かを判定する。

#### 【0225】

ステップ S2402 において、NO である場合、すなわち、コンテンツの送出が完了していない場合には、ステップ S2403 を実行する。

ステップ S2402 において、YES である場合、すなわち、コンテンツの送出が全て完了した場合には、その旨をコンテンツ取得要求受信手段 901 に通知する等を行い、本処理を終了する。

#### 【0226】

コンテンツ取得手段 902 は、コンテンツ DB 903 から、該当コンテンツ ID のコンテンツを読み出す（ステップ S2403）。具体的には、コンテンツ取得手段 902 は、コンテンツ取得要求受信手段 901 から受け取ったコンテンツ ID をキーとしてコンテンツ DB 903 を検索し、該当コンテンツを取得する。

#### 【0227】

コンテンツ取得手段 902、および、コンテンツ多重化手段 904 は、それぞれ、PES パケット 1000、および、TS パケット 1100 を順次生成する（ステップ S2404）。具体的には、コンテンツ取得手段 902 は、ステップ S2403 においてコンテンツ DB 903 から取得したコンテンツの映像、音声な

どを順次MPEGエンコードし、第1の時刻情報付与手段908から取得したSTCを用いて、映像ES、音声ESの同期を実現するためのPTS1043a、DTS1043bを付与する。

#### 【0228】

また、コンテンツ多重化手段904は、コンテンツ取得手段902から取得したPESパケット1000をTSパケット化する。このとき、第1の時刻情報付与手段908から取得したSTCを用いて、端末装置102内の基準クロックを、コンテンツ配信サーバ101cの基準クロック（計時手段907）と同期させるためのPCR1125aを付与する。さらに、PCR1125aの改ざんを防止するため、PCR1125aとTSパケット1100のペイロード部（TSP Payload1130）とのハッシュを計算し、TSパケット1100のプライベートデータ部（Private Data1125e）に挿入する。さらに、コンテンツ多重化手段904は、PSI（PAT、PMTなど）、ヌルパケット等のその他のTSパケット1100も生成し、コンテンツのTSパケット1100と共に多重する。

#### 【0229】

第1の時刻情報付与手段908は、コンテンツ多重化手段904において処理しているTSパケット1100が、コンテンツの先頭のTSパケット1100であるかどうかを判定する（ステップS2405）。具体的には、第1の時刻情報付与手段908は、TSパケット1100のPrivate Data1125eに設定されている、コンテンツ開始を示すフラグを監視し、当該フラグが設定されたTSパケット1100を検出する。

#### 【0230】

ステップS2405において、YESである場合、すなわち、処理中のTSパケット1100がコンテンツの先頭のTSパケット1100である場合には、ステップS2406を実行する。

#### 【0231】

ステップS2405において、NOである場合、すなわち、処理中のTSパケット1100がコンテンツの先頭のTSパケット1100でない場合には、ステ

ップ S 2 4 0 7 を実行する。

#### 【0232】

第2の時刻情報記録手段909は、第1の時刻情報付加手段908から受け取った第2の時刻情報を記録する（ステップS 2 4 0 6）。具体的には、第2の時刻情報記録手段909は、第1の時刻情報付加手段908がステップS 2 4 0 5において、コンテンツの先頭のTSパケット1100を検出した時点でのPCR 1125a（STC）の値を第2の時刻情報として受信するので、この第2の時刻情報を内部で保持する。なお、このように取得した第2の時刻情報は、LAN 101nを通じて即座に利用実績収集サーバ101eに送信しても良いし、利用実績収集サーバ101eから要求された時点で、利用実績収集サーバ101eに送信するようにしても良いし、適当なタイミングで利用実績収集サーバ101eに送信するようにしても良い。

#### 【0233】

コンテンツ暗号化手段905、および、コンテンツ送出手段910は、TSパケット1100をコンテンツ鍵で暗号化した後、RTPパケットを生成して端末装置102に送信する（ステップS 2 4 0 7）。具体的には、コンテンツ暗号化手段905は、コンテンツ多重化手段904から受信したTSパケット1100のペイロード部（TS P Payload 1130）を、コンテンツ鍵供給手段906から受け取ったコンテンツ鍵で暗号化する。

#### 【0234】

また、コンテンツ鍵供給手段906は、コンテンツ取得要求受信手段901から、端末装置102に送出するコンテンツのコンテンツIDを受け取り、対応するコンテンツ鍵をコンテンツ鍵DB 911から読み出し、コンテンツのPIDと共にコンテンツ暗号化手段905に渡す。なお、このときのコンテンツのPIDは、コンテンツ暗号化手段905が暗号化するTSパケット1100を特定するために用い、コンテンツ多重化手段904から指示されたPIDを渡すという処理を行う。

#### 【0235】

また、コンテンツ送出手段910は、コンテンツ暗号化手段905から受け取

った暗号化されたTSパケット1100を、一定サイズで分割（または集約）してRTPヘッダを付加し、RTPパケットを生成して端末装置102に順次伝送する。その後、ステップS2402を実行する。

#### 【0236】

以上、端末装置102でストリーミングコンテンツを利用する際の、コンテンツ配信サーバ101cにおけるコンテンツの送出手続きについての説明を終了する。

#### 【0237】

次に、端末装置102において記録したコンテンツの利用実績を、UL1700を用いて利用実績収集サーバ101eに送信する動作を、図25に示すフローチャートを用いて説明する。

#### 【0238】

端末装置102の利用実績送信手段1506は、利用実績収集サーバ101eに送信すべき利用実績（UL1700）をセキュアDB1504から取得する（ステップS2501）。具体的には、利用実績送信手段1506は、セキュアDB1504中の全てのLT700を検索して、利用実績収集指示タグブロック704の指示情報803内の利用実績返却条件813を参照する。ここで、利用実績の返却条件を満たしている場合には、LT700中のライセンスID712と一致するライセンスID1706を有するUL1700をセキュアDB1504から取得する。

#### 【0239】

利用実績送信手段1506は、ステップS2501の結果、利用実績収集サーバ101eに送信するUL1700の有無を確認する（ステップS2502）。

ステップS2502において、YESである場合、すなわち、利用実績収集サーバ101eに送信するUL1700が存在する場合には、ステップS2503を実行する。

#### 【0240】

ステップS2502において、NOである場合、すなわち、利用実績収集サーバ101eに送信するUL1700が存在しない場合には、本処理を終了する。

利用実績送信手段1506は、利用実績収集サーバ101eに対して、利用実績を送信する（ステップS2503）。具体的には、利用実績送信手段1506は、第2の送受信手段1501を通じて、UL1700を利用実績収集サーバ101eに送信する。このとき、端末装置102と利用実績収集サーバ101eとは、SSLなどによりSACを確立してから、UL1700を送信する。なお、端末装置102と利用実績収集サーバ101eとが、互いに予め共有する暗号鍵を用いて、UL1700を暗号化することにより、UL1700のセキュリティを確保することも可能である。なお、UL1700の送信において、SAC等の方法を用いることにより、UL1700の送信元の特定が可能となる。

#### 【0241】

利用実績収集サーバ101eにおける第1の時刻情報取得手段1201は、端末装置102から第1の時刻情報を利用実績として受信する（ステップS2504）。具体的には、第1の時刻情報取得手段1201は、ネットワーク103を通じて、端末装置102からUL1700を受信する。

#### 【0242】

利用実績取得手段1203は、第1の時刻情報と第2の時刻情報とから、ユーザがコンテンツのどの部分を利用したかを算出する（ステップS2505）。具体的には、端末装置102から受信したUL1700に設定された第1の時刻情報と、コンテンツ配信サーバ101cから受信した第2の時刻情報との差分を計算し、コンテンツ内の利用部分を特定するための情報を取得する。例えば、UL1700の時刻情報1710の開始時刻情報および終了時刻情報が、それぞれ、「13970584」および「13999999」である場合に、第2の時刻情報が「10000000」であった場合には、コンテンツ内の利用部分は、第1の時刻情報の値から第2の時刻情報の値を減算することにより、それぞれ、「3970584」および「3999999」と算出される。

#### 【0243】

なお、第2の時刻情報については、必要となった時点でコンテンツ配信サーバ101cに要求し、第2の時刻情報を取得するようにしても良いし、利用実績収集サーバ101eが、コンテンツ配信サーバ101cから予め取得して管理して

おくようにしても良い。

#### 【0244】

利用実績取得手段1203は、ステップS2505で算出したコンテンツの利用部分、および、ユーザID、コンテンツID等の利用実績として必要な情報を、利用実績DB1204に蓄積する（ステップS2506）。具体的には、利用実績取得手段1203は、ステップS2505で算出した、コンテンツの利用開始および終了の時刻（コンテンツの開始からの相対時刻）である「3970584」および「3999999」を利用実績管理テーブル1400の利用実績1405に記録する。同時に、図14に示した、ユーザID1401、端末ID1402、コンテンツID1403、ライセンスID1404も蓄積する。また、UL1700のアクション種別1707、あるいは、利用開始時刻1708が設定されていた場合には、利用実績管理テーブル1400の利用実績1405に設定する。

#### 【0245】

第1の時刻情報取得手段1201は、UL1700の受信完了通知を端末装置102に送信する（ステップS2507）。

端末装置102の利用実績送信手段1506は、利用実績収集サーバ101eからのUL1700の受信完了通知を受信した時点で、送信したセキュアDB1504を更新（コミット）することにより、利用実績収集サーバ101eに送信したUL1700を完全に削除する（ステップS2508）。

#### 【0246】

以上、端末装置102が利用実績収集サーバ101eにUL1700を送信する動作について説明した。

以上のように、コンテンツ利用実績収集システム1では、配信センター101において生成した第1の時刻情報をセキュアにバインドして端末装置102に配信すると共に、コンテンツの先頭での第1の時刻情報を第2の時刻情報として配信センター101で保持し、利用実績の収集後に配信センター101において、端末装置102から利用実績として収集した第1の時刻情報と、配信センター101が保持する第2の時刻情報とから、ユーザがコンテンツのどの部分を利用し

たかを算出している。そのため、コンテンツプロバイダ、サービスプロバイダは、詳細かつセキュアにユーザの利用実績を取得することができる。

#### 【0247】

##### (実施の形態2)

以下、本発明における実施の形態2について、図面を用いて詳細に説明する。

本発明における実施の形態2で説明するコンテンツ利用実績収集システム2は、コンテンツ利用実績収集システム1において、コンテンツの先頭での第1の時刻情報を第2の時刻情報として配信センター101で保持し、利用実績の収集後に配信センター101において、コンテンツの利用部分を算出するようにしていたのに対し、第1の時刻情報と第2の時刻情報とをコンテンツに付与し、端末装置102において、コンテンツの利用部分を算出するようにしている。なおコンテンツ利用実績収集システム2の全体の概略構成に関しては、コンテンツ利用実績収集システム1と同様であるので、ここでは説明を省略する。また、本発明における実施の形態1と同様の構成要素については、実施の形態1において既に説明しているので、以下の説明を省略する。

#### 【0248】

以下、配信センター101のコンテンツ配信サーバ101cについて、図26を用いて説明を行う。本図において、図9に示した実施の形態1のコンテンツ配信サーバ101cと同様の構成要素については、図9において既に説明しているので、図9と同様の符号を付して以下の説明を省略する。

#### 【0249】

図26に示すコンテンツ配信サーバ101cは、図9における第1の時刻情報付加手段908に代わり、時刻情報付加手段2601を有し、第2の時刻情報記録手段909を有さない構成となっている。

#### 【0250】

時刻情報付加手段2601は、コンテンツに第1の時刻情報と第2の時刻情報とを付加する手段である。具体的には、時刻情報付加手段2601は、計時手段907から第1の時刻情報(STC)を取得し、コンテンツ取得手段902およびコンテンツ多重化手段904に対して、それぞれ、PESパケット1000の

P T S 1 0 4 3 a / D T S 1 0 4 3 b、および、T S パケット 1 1 0 0 の P C R 1 1 2 5 a のためのタイムスタンプを付与する。この処理については、本発明の実施の形態 1 におけるコンテンツ配信サーバ 1 0 1 c の処理と同様である。さらに、時刻情報付加手段 2 6 0 1 は、本発明の実施の形態 1 におけるコンテンツ配信サーバ 1 0 1 c と同様の手法で、コンテンツ開始の第 1 の時刻情報（すなわち、P C R、S T C）の値を第 2 の時刻情報として取得し、コンテンツ多重化手段 9 0 4 に提供する処理を行う。

#### 【0251】

コンテンツ多重化手段 9 0 4 は、本発明の実施の形態 1 に示したコンテンツ多重化手段 9 0 4 における第 1 の時刻情報の付加処理（P C R 1 1 2 5 a の値の設定）に加え、時刻情報付加手段 2 6 0 1 から取得した第 2 の時刻情報を T S パケット 1 1 0 0 の P r i v a t e D a t a 1 1 2 5 e に設定する。なお、P r i v a t e D a t a L e n g t h 1 1 2 5 d は、追加した第 2 の時刻情報の長さに応じて、適切な値が設定される。また、本発明の実施の形態 1 で示した、ハッシュ値の計算処理および P r i v a t e D a t a 1 1 2 5 e へのハッシュ値の付加処理は行われない。

#### 【0252】

コンテンツ暗号化手段 9 0 5 は、コンテンツの暗号化方法を除いて、本発明の実施の形態 1 におけるコンテンツ暗号化手段 9 0 5 と同様の処理を行う。P C R 1 1 2 5 a（第 1 の時刻情報）および P r i v a t e D a t a 1 1 2 5 e に付加された第 2 の時刻情報は、T S パケット 1 1 0 0 の非暗号化部に存在するため、第 1 の時刻情報あるいは第 2 の時刻情報の値が不正に改ざんされ、配信センター 1 0 1 において正しい利用実績が取得できない恐れがある。そこで、コンテンツ暗号化手段 9 0 5 は、コンテンツ鍵 D B 9 1 1 で管理されるコンテンツ毎のコンテンツ鍵と、第 1 の時刻情報である P C R 1 1 2 5 a と、第 2 の時刻情報とを組み合わせ、T S P P a y l o a d 1 1 3 0 の暗号鍵として用いる。これにより、T S パケット 1 1 0 0 の非暗号化部に設定された第 1 の時刻情報あるいは第 2 の時刻情報が不正に改ざんされた場合、端末装置 1 0 2 は正しい暗号鍵を生成することができないので、結果としてコンテンツの復号処理が失敗し、第 1 の時

刻情報および第2の時刻情報の改ざんを防止することができる。すなわち、コンテンツ暗号化手段905は、第1の時刻情報および第2の時刻情報と、コンテンツとを、セキュアにバインドするための手段であるとも言える。

#### 【0253】

時刻情報とコンテンツ鍵との組み合わせ方法については、第1の時刻情報および第2の時刻情報が秘匿情報でないため、簡単な方法を用いても良く、例えば、コンテンツ鍵と第1の時刻情報と第2の時刻情報とのXOR (Exclusive OR) の値を、TSP Payload1130の暗号鍵として用いる方法などが挙げられる。あるいは、TSP Payload1130の暗号化モードがCBCなどの初期ベクトルを必要とするモードである場合は、少なくとも第1の時刻情報と第2の時刻情報とを含む情報を初期ベクトルとして用いることにより、第1の時刻情報および第2の時刻情報を含むTSパケット1100毎に拡大鍵を生成する手間を削減することができる。

#### 【0254】

なお、第1の時刻情報と第2の時刻情報とコンテンツ鍵とを組み合わせる暗号鍵を生成する処理は、PCR1125a (およびPrivate Data1125eの第2の時刻情報) が設定されたTSパケット1100に対してのみ行う。

また、ここでは、TSパケット1100に第1の時刻情報と第2の時刻情報とが設定される場合において、2つの時刻情報をコンテンツ鍵と組み合わせる例を示したが、これに限られるものではなく、TSパケット1100の非暗号化部に設定された時刻情報が1つのみである場合にも適用することができる。

#### 【0255】

以上、配信センター101のコンテンツ配信サーバ101cについての説明を終了する。

次に、配信センター101の利用実績収集サーバ101eについて、図27を用いて説明する。

#### 【0256】

本発明の実施の形態2における利用実績収集サーバ101eは、図12に示し

た利用実績収集サーバ101eの第1の時刻情報取得手段1201および第2の時刻情報取得手段1202を有さず、利用実績取得手段1303と、利用実績DB1304とから構成されている。

#### 【0257】

利用実績取得手段1303は、端末装置102から利用実績を受信する。具体的には、利用実績取得手段1303は、ネットワーク103を介して、端末装置102からUL1700を受信し、UL1700に設定された利用実績を利用実績DB1304に蓄積する。本発明の実施の形態1では、UL1700に設定された利用実績である第1の時刻情報と、コンテンツ配信サーバ101cで管理されている第2の時刻情報とから、コンテンツの利用部分を算出する処理を行ったが、本発明の実施の形態2では、端末装置102においてコンテンツの利用部分を算出する処理を行うようにしているため、基本的にはUL1700の内容をそのまま蓄積するだけの処理が行われる。

#### 【0258】

また、利用実績DB1304は、図14に示した利用実績管理テーブル1400と同様のテーブルを管理するので、ここでは説明を省略する。

以上、配信センター101の利用実績収集サーバ101eについての説明を終了する。

#### 【0259】

次に、コンテンツ利用実績収集システム2における端末装置102の構成について説明する。図28は、図1に示される端末装置102の詳細な構成を示す機能ブロック図である。

#### 【0260】

図28は、図15に示した端末装置102の第1の時刻情報記録手段1523に代わり、時刻情報算出手段2801を備えている。なお、その他の手段については、コンテンツ復号手段1521およびコンテンツ利用手段1522を除き、本発明の実施の形態1における説明と同様であるので、ここでは省略する。

#### 【0261】

時刻情報算出手段2801は、コンテンツ復号手段1521において取得した

第1の時刻情報および第2の時刻情報を受信し、第1の時刻情報と第2の時刻情報とから、コンテンツの利用部分を特定するための時刻情報（すなわち、コンテンツの先頭からの相対時刻）を算出し、記録する。具体的には、時刻情報算出手段2801は、コンテンツ復号手段1521から、コンテンツの利用開始時および利用終了時の第1の時刻情報を取得すると共に、コンテンツの開始時の第1の時刻情報の値である第2の時刻情報を取得し、第2の時刻情報の値から第1の時刻情報の値を減算する処理を行い、その結果をコンテンツの利用部分を特定する時刻情報として記録する。つまり、図13を用いて説明すると、本発明の実施の形態1では、利用実績収集サーバ101eが第2の時刻情報の値（PCR\_\_T）を保持しておき、利用実績収集サーバ101eで、（PCR\_\_S-PCR\_\_T）および（PCR\_\_E-PCR\_\_T）を算出していたが、本発明の実施の形態2では、TSパケット1100で第2の時刻情報（PCR\_\_T）を配信しているので、端末装置102の時刻情報算出手段2801で、（PCR\_\_S-PCR\_\_T）および（PCR\_\_E-PCR\_\_T）を算出することができる。

#### 【0262】

コンテンツ復号手段1521は、図15に示したコンテンツ復号手段1521と基本的に同様の処理を行う手段であるが、コンテンツの復号方法と、コンテンツに設定された時刻情報の取得方法とが異なる。具体的には、コンテンツ復号手段1521は、TSパケット1100のAdaptation\_field1120から、PCR1125a、および、Private\_Data1125eに設定された第1の時刻情報、および、第2の時刻情報を取得する。これらの時刻情報と、コンテンツ利用制御手段1503から取得するコンテンツ鍵とからTSパケット1100の復号鍵を生成し（例えば、XORするなど）、暗号化されているペイロード（TSP\_Payload1130）を復号する。なお、PCR1125aは全てのTSパケット1100に含まれているとは限らないため、PCR1125aが設定されたTSパケット1100についてのみ、時刻情報とコンテンツ鍵とから復号鍵を生成する処理を行う。

#### 【0263】

また、ユーザの操作が行われた時点での第1の時刻情報と第2の時刻情報とを

時刻情報算出手段 2801 に送信する。但し、有効な利用実績のみを記録するため、コンテンツ利用手段 1522 からデコード処理失敗や、特殊再生中であるといったデコードのステータスの通知を受け取った場合には、時刻情報算出手段 2801 に対して第 1 の時刻情報と第 2 の時刻情報とを送信しない処理を行う。なお、デコード処理の失敗のログや特殊再生中の利用実績を取得したい場合には、時刻情報算出手段 2801 に対して、デコードのステータスと共に第 1 の時刻情報と第 2 の時刻情報とを送信するようにしても良い。

#### 【0264】

コンテンツ利用手段 1522 は、図 15 に示したコンテンツ利用手段 1522 と基本的に同様の処理を行う手段であるが、デコード処理を行った結果（ステータスなど）を、コンテンツ復号手段 1521 に通知する処理を行う点が異なる。具体的には、コンテンツの非暗号化部に設定された第 1 の時刻情報あるいは第 2 の時刻情報が改ざんされた場合、コンテンツ復号手段 1521 から受信した TS パケット 1100 に設定された映像 ES、音声 ES などのデコードに失敗するため、コンテンツ利用手段 1522 は、その旨をコンテンツ復号手段 1521 に通知する処理を行う。また、早送り、巻戻しなどの特殊再生が行われた場合、その旨をコンテンツ復号手段 1521 に通知することによって、コンテンツ復号手段 1521 や時刻情報算出手段 2801 などは、特殊再生が行われていることを認識して、利用実績を記録するか否かを決定することができる。

#### 【0265】

以上、図 28 を用いて、端末装置 102 の構成についての説明を行った。

以上のように構成された端末装置 102 において、ユーザが権利管理サーバ 101b から LT700 を取得してセキュアにコンテンツを利用し、第 1 の時刻情報と第 2 の時刻情報とから算出した、コンテンツの先頭からの相対時刻である利用実績を記録し、利用実績を端末装置 102 から利用実績収集サーバ 101e に送信する、という一連の動作を、図 29～図 31 に示すフローチャートを用いて説明する。なお、端末装置 102 における権利管理サーバ 101b からの LT700 の取得処理、端末装置 102 におけるコンテンツ利用処理および利用実績記録処理の全体処理については、それぞれ、本発明の実施の形態 1 における図 18

～図21の処理と同様であるため、ここでは省略する。また、端末装置102における利用実績収集サーバ101eに対する利用実績送信処理については、端末装置102で記録した利用実績を利用実績収集サーバ101eに送信し、利用実績収集サーバ101eが利用実績を利用実績DB1304に蓄積する処理のみであるため、ここでは省略する。

#### 【0266】

よって、ここでは、コンテンツ利用処理および利用実績記録処理の詳細処理、および、コンテンツ配信サーバ101cにおけるストリーム送出処理についてのみ、それぞれ、図29および図30、図31を用いて説明する。

#### 【0267】

まず、ステップS2108のコンテンツ利用処理および利用実績記録処理について、図29および図30は端末装置102におけるコンテンツ利用処理および利用実績記録処理を、図31は、コンテンツ配信サーバ101cにおけるコンテンツ利用処理を示している。

#### 【0268】

最初に、端末装置102におけるコンテンツ利用処理および利用実績記録処理について、図29を用いて説明する。

コンテンツ利用手段1522は、コンテンツ配信サーバ101cに対して、コンテンツ取得要求を送信する（ステップS2901）。具体的には、コンテンツ利用手段1522は、端末アプリケーション1550から受信したコンテンツのURIを基にコンテンツ配信サーバ101cに接続し、RTSPを用いて再生要求（PLAY）を送信する。コンテンツ配信サーバ101cは、対応するコンテンツをRTPのペイロードに設定して端末装置102に対して順次送信する。

#### 【0269】

第2の送受信手段1501は、コンテンツ配信サーバ101cからコンテンツを受信する（ステップS2902）。具体的には、第2の送受信手段1501は、コンテンツ配信サーバ101cが送信したRTPパケットを順次受信し、RTPペイロードから順次MP EG-2 TSを取り出し、コンテンツ復号手段1521に対して送信する。

**【0270】**

第2の送受信手段1501は、コンテンツ配信サーバ101cからのコンテンツ受信が完了したか否かを判定する（ステップS2903）。具体的には、第2の送受信手段1501は、受信したRTPパケットが最終パケットであるか等の方法により、ストリームの終端を検出する。

**【0271】**

ステップS2903において、NOである場合、すなわち、コンテンツの受信が完了していない場合には、ステップS2904を実行する。

ステップS2903において、YESである場合、すなわち、ユーザから端末アプリケーション1550を通じて、コンテンツ利用終了の通知を受けた場合や、コンテンツの受信が完了した場合には、端末アプリケーション1550を通じてその旨をユーザに通知し、本処理を終了する。

**【0272】**

コンテンツ復号手段1521は、TSパケット1100毎にコンテンツ復号のための復号鍵を生成し、TSパケット1100を復号すると共に、コンテンツ利用手段1522は、コンテンツをデコードする（ステップS2905）。具体的には、コンテンツ復号手段1521は、第2の送受信手段1501から受信したTSパケット1100の内、ペイロード部（TSP Payload1130）が暗号化されているTSパケット1100の復号を行う。この際、処理中のTSパケット1100がPCR1125aを含んでいる場合には、コンテンツ利用制御手段1503から受信したコンテンツ鍵と、PCR1125a（第1の時刻情報）と、Private Data1125eの第2の時刻情報とをXORすることにより、コンテンツの復号鍵を生成する。PCR1125aを含んでいない場合には、コンテンツ利用制御手段1503から受信したコンテンツ鍵を用いてTSパケット1100のペイロード部（TSP Payload1130）を復号する。なお、TSパケット1100がPCR1125aを含んでいるか否かについては、Adaptation Field1120のPCR\_Flag1124を参照することにより判別可能である。

**【0273】**

ペイロードが復号されたTSパケット1100は、コンテンツ利用手段1522に渡され、順次デコードされる。

なお、このとき、非暗号化部に存在する第1の時刻情報または第2の時刻情報が改ざんされている場合には、コンテンツ復号手段1521は、正しいコンテンツの復号鍵が生成できないためにコンテンツの復号に失敗し、その結果、コンテンツ利用手段1522はコンテンツのデコードに失敗する。この場合のデコード失敗のステータスを、コンテンツ復号手段1521に通知するようにしても良い。これにより、コンテンツ復号手段1521は、コンテンツのデコードに失敗した場合の利用実績を記録しないようにすることができる。あるいは、コンテンツのデコードに失敗した旨を、利用実績として記録することもできる。

#### 【0274】

次に、図29におけるステップS2904に示した、利用実績記録処理について、図30を用いて説明する。

コンテンツ復号手段1521は、PCR1125aの値を一時記録する（ステップS3001）。具体的には、コンテンツ復号手段1521は、PCR1125aが設定されているTSパケット1100を処理した場合、PCR1125aの値を取得して、内部で一時的に記録する。なお、このとき、Private Data1125eの第2の時刻情報も取得し、内部で一時的に記録するようにしても良い。

#### 【0275】

コンテンツ復号手段1521は、コンテンツ利用手段1522からの状態通知を受信したか否かをチェックする（ステップS3002）。具体的には、コンテンツ復号手段1521は、コンテンツ利用手段1522からの再生、停止、早送り、巻戻しなどや、コンテンツのデコード失敗などのデコードの状態を受信する。

#### 【0276】

ステップS3002において、YESである場合、すなわち、コンテンツ利用手段1522からの状態通知を受信した場合には、ステップS3003を実行する。

**【0277】**

ステップS3002において、NOである場合、すなわち、コンテンツ利用手段1522からの状態通知を受信していない場合には、ステップS3001を実行する。

**【0278】**

コンテンツ復号手段1521は、コンテンツ利用手段1522からの状態通知に応じて、第1の時刻情報および第2の時刻情報を時刻情報算出手段2801に送信し、時刻情報算出手段2801が開始時刻情報または終了時刻情報を算出する（ステップS3003）。具体的には、コンテンツ復号手段1521は、コンテンツ利用手段1522からのデコードの状態通知に応じて、一時記録した第1の時刻情報とTSパケット1100のPrivate Data1125eの第2の時刻情報とを取得し、時刻情報算出手段2801に通知する。時刻情報算出手段2801は、第1の時刻情報と第2の時刻情報との差分を計算して、コンテンツを視聴した部分を特定する利用実績を生成する。例えば、コンテンツ利用手段1522から「再生開始」を受け取った場合には、開始時刻情報として利用実績を記録し、「早送り」を受け取った場合には、終了時刻情報として利用実績を記録する処理を行う。

**【0279】**

コンテンツ復号手段1521は、コンテンツ利用手段1522からの状態通知が「コンテンツ利用終了」、すなわち「停止」であるかどうかを判定する（ステップS3004）。

**【0280】**

ステップS3004において、YESである場合、すなわち、コンテンツ利用手段1522からの状態通知が「停止」である場合には、このとき、記録した利用実績（開始時刻情報および終了時刻情報）を、利用実績記録手段1505に送信して、本処理を終了する。なお、記録した利用実績を、利用実績記録手段1505に送信するタイミングはコンテンツ利用終了時に限らず、例えば、ユーザ操作が行われる都度（利用実績が記録される都度）や、一定時間間隔で送信するようにしても良い。

**【0281】**

ステップS3004において、NOである場合、すなわち、コンテンツ利用手段1522からの状態通知が「停止」以外である場合には、ステップS3001を実行する。

**【0282】**

次に、端末装置102のコンテンツ利用時における、コンテンツ配信サーバ101cのコンテンツ送信処理について、図31を用いて説明する。

コンテンツ配信サーバ101cにおけるコンテンツ取得要求受信手段901は、端末装置102からのコンテンツ取得要求を受信する（ステップS3101）。具体的には、コンテンツ取得要求受信手段901は、端末装置102からRTSPによって再生要求を受け、要求されたコンテンツIDを取得して、コンテンツIDをコンテンツ取得手段902に送信する。

**【0283】**

時刻情報付加手段2601は、第2の時刻情報を一時的に保持する（ステップS3102）。具体的には、時刻情報付加手段2601は、コンテンツ取得手段902からのコンテンツ読み出しを開始する旨の通知を受信すると、STCの値を計時手段907から取得し、コンテンツの先頭での第1の時刻情報、すなわち、第2の時刻情報として、時刻情報付加手段2601の内部で保持する。なお、時刻情報付加手段2601は、その後も継続的に計時手段907からのSTCを取得して、コンテンツ取得手段902およびコンテンツ多重化手段904に供給する処理を行う。

**【0284】**

コンテンツ送出手段910は、コンテンツの送出が完了したか否かを判定する（ステップS3103）。具体的には、コンテンツ送出手段910は、コンテンツの全てをRTPパケットとして端末装置102に送出したか否かを判定する。

**【0285】**

ステップS3103において、NOである場合、すなわち、コンテンツの送出が完了していない場合には、ステップS3104を実行する。

ステップS3103において、YESである場合、すなわち、コンテンツの送

出が全て完了した場合には、その旨をコンテンツ取得要求受信手段 901 に通知する等を行い、本処理を終了する。

#### 【0286】

コンテンツ取得手段 902 は、コンテンツ DB 903 から、該当コンテンツ ID のコンテンツを読み出す（ステップ S3104）。具体的には、コンテンツ取得手段 902 は、コンテンツ取得要求受信手段 901 から受け取ったコンテンツ ID をキーとしてコンテンツ DB 903 を検索し、該当コンテンツを取得する。

#### 【0287】

コンテンツ取得手段 902、および、コンテンツ多重化手段 904 は、それぞれ、PES パケット 1000、および、TS パケット 1100 を順次生成すると共に、TS パケット 1100 に第 1 の時刻情報および第 2 の時刻情報を付加する（ステップ S3105）。具体的には、コンテンツ取得手段 902 は、ステップ S3104 においてコンテンツ DB 903 から取得したコンテンツの映像、音声などを順次 MPEG エンコードし、時刻情報付加手段 2601 から取得した STC を用いて、映像 ES、音声 ES の同期を実現するための PTS 1043a、DTS 1043b を付与する。

#### 【0288】

また、コンテンツ多重化手段 904 は、コンテンツ取得手段 902 から取得した PES パケット 1000 を TS パケット化する。このとき、時刻情報付加手段 2601 から取得した STC を用いて、端末装置 102 内の基準クロック（図 28 に図示しない STC）を、コンテンツ配信サーバ 101c の基準クロック（STC、すなわち、計時手段 907）と同期させるための PCR 1125a を付与すると共に、Private Data 1125e に一時保持しておいた第 2 の時刻情報を付与する。さらに、コンテンツ多重化手段 904 は、PSI（PAT、PMT など）、ヌルパケット等のその他の TS パケット 1100 も生成し、コンテンツの TS パケット 1100 と共に多重する。

#### 【0289】

コンテンツ暗号化手段 905、および、コンテンツ送出手段 910 は、TS パケット 1100 をコンテンツ鍵で暗号化した後、RTP パケットを生成して端末

装置 102 に送信する (ステップ S3106)。具体的には、コンテンツ暗号化手段 905 は、コンテンツ多重化手段 904 から受信した TS パケット 1100 に PCR1125a が含まれている場合には、第 1 の時刻情報 (PCR1125a) と、Private Data1125e の第 2 の時刻情報と、コンテンツ鍵供給手段 906 から受け取ったコンテンツ鍵の XOR によりペイロードを暗号化する暗号鍵を生成し、TS パケット 1100 のペイロード部 (TSP Payload1130) を暗号化する。TS パケット 1100 に PCR1125a が含まれていない場合には、コンテンツ鍵供給手段 906 から受け取ったコンテンツ鍵のみを用いて、TS パケット 1100 のペイロード部 (TSP Payload1130) を暗号化する。

#### 【0290】

また、コンテンツ鍵供給手段 906 は、コンテンツ取得要求受信手段 901 から、端末装置 102 に送出するコンテンツのコンテンツ ID を受け取り、対応するコンテンツ鍵をコンテンツ鍵 DB911 から読み出し、コンテンツの PID と共にコンテンツ暗号化手段 905 に渡す。なお、このときのコンテンツの PID は、コンテンツ暗号化手段 905 が暗号化する TS パケット 1100 を特定するために用い、コンテンツ多重化手段 904 から指示された PID を渡すという処理を行う。

#### 【0291】

また、コンテンツ送出手段 910 は、コンテンツ暗号化手段 905 から受け取った暗号化された TS パケット 1100 を、一定サイズで分割 (または集約) して RTP ヘッダを付加し、RTP パケットを生成して端末装置 102 に順次伝送する。その後、ステップ S3103 を実行する。

#### 【0292】

以上、端末装置 102 でストリーミングコンテンツを利用する際の、コンテンツ配信サーバ 101c におけるコンテンツの送出を行う動作についての説明を終了する。

#### 【0293】

以上のように、コンテンツ利用実績収集システム 2 では、配信センター 101

において生成した第1の時刻情報と、コンテンツの先頭での第1の時刻情報である第2の時刻情報とをセキュアにバインドして端末装置102に配信し、端末装置102において、第1の時刻情報と第2の時刻情報とから、ユーザがコンテンツのどの部分を利用したかを算出している。そのため、コンテンツプロバイダ、サービスプロバイダは、詳細かつ安全にユーザの利用実績を取得することができると共に、利用実績収集時の利用実績収集サーバ101eの処理を削減することができる。また、コンテンツ配信サーバ101cと利用実績収集サーバ101eとの間で、第2の時刻情報をやり取りするための仕組みが不要となり、配信センター101のシステムの柔軟性が高まる。

#### 【0294】

なお、本発明における実施の形態では、TSパケット1100のPCR1125a、および、Private Data1125eに、第1の時刻情報および第2の時刻情報を設定する場合の例を示したが、これに限られるものではなく、PESパケット1000のPTS1043a、DTS1043bや、PES Private Data1081を用いて、第1の時刻情報、第2の時刻情報など、コンテンツの利用部分を特定可能な時刻情報を設定するようにしても良い。あるいは、MPEG-2 PS (Program Stream) やMPEG-4システムのSL (Sync Layer) の時刻情報を用いたり、PESレイヤよりも下位のMPEG-2、MPEG-4などのESレイヤ中の時刻情報（例えば、MPEG-2 ESのGroup Of PictureのTime Codeなど）を用いるようにしても良い。

#### 【0295】

この場合、PESパケット1000そのものが、適当なサイズに分割されて、TSパケット1100のTSP Payload1130に設定されて暗号化されるため、PESパケット1000内の時刻情報（PTS1043a、DTS1043b、PES Private Data1081に設定した時刻情報）はセキュアにコンテンツにバインドされる。ゆえに、コンテンツ配信サーバ101cにおいて、コンテンツ（TSパケット1100）の暗号化処理以外に、第1の時刻情報や第2の時刻情報をコンテンツにセキュアにバインドするための特別な

処理が不要になるため、コンテンツ配信サーバ 101c の負担が軽減されるという効果がある。

#### 【0296】

また、本発明における実施の形態では、端末装置 102 で利用実績として記録した第 1 の時刻情報と、第 2 の時刻情報とから、利用実績収集サーバ 101e または端末装置 102 において、コンテンツの利用部分を特定可能な、コンテンツの先頭からの相対時刻を算出する場合の例を示したが、コンテンツ配信サーバ 101c において、予め第 1 の時刻情報と第 2 の時刻情報とから、コンテンツの先頭からの相対時刻を計算しておき、これをコンテンツに設定することによって、端末装置 102 ではコンテンツに設定された時刻情報をそのまま記録するようにしても良い。これによれば、端末装置 102 における利用実績記録処理、および、利用実績収集サーバ 101e での利用実績収集処理の負荷を軽減することができる。

#### 【0297】

このとき、前記コンテンツの先頭からの相対時刻は、PES パケット 1000 の PES Private Data 1081、あるいは、TS パケット 1100 の Private Data 1125e などに設定することが可能である。また、前記コンテンツの先頭からの相対時刻を、TS パケット 1100 の Private Data 1125e に設定する場合は、前述した方法を用いて、TS パケット 1100 のペイロード部 (TSP Payload 1130) にセキュアにバインドしても良い。また、PCR 1125a、PTS 1043a/DTS 1043b といった時刻情報は、STC の再生やコンテンツのデコード、再生のために必須であるため、TS パケット 1100 および PES パケット 1000 に付加されるのは言うまでもない。ゆえに、本発明の実施の形態 1 および実施の形態 2 において説明した、特殊再生時における利用実績記録処理は、この場合にも適用可能である。

#### 【0298】

また、本発明における実施の形態では、配信センター 101 において、コンテンツの先頭の PCR 1125a の値 (第 2 の時刻情報) を記録するようにしたが

、少なくとも第2の時刻情報の値があれば良いため、例えば、コンテンツの全てのPCR1125aの値を記録したマップを記録するようにしても良い。また、このマップを端末装置102に送信して、端末装置102で、このマップを用いてコンテンツの利用部分を特定する情報を生成するようにしても良い。すなわち、本発明における実施の形態では、利用実績を記録するための時刻情報をコンテンツに設定する例を示したが、これに限られるものではなく、コンテンツとは別に配信するようにしても良い。他の例としては、MPEG-2 SystemsのPrivate Sectionを用い、プライベートストリーム(ES)として時刻情報を配信する方法が考えられる。このとき、時刻情報とコンテンツとをセキュアにバインドするようにしても良い。

#### 【0299】

また、本発明における実施の形態では、コンテンツ配信サーバ101cからコンテンツがストリーミング配信される場合の例を示したが、これに限られるものではなく、端末装置102内あるいはネットワーク103上の記録手段に蓄積されたダウンロードコンテンツ(ストリーミングコンテンツの蓄積も含む)であっても良い。

#### 【0300】

また、本発明における実施の形態では、利用実績であるUL1700にLT700を特定するためのIDであるライセンスID1706を設定するようにしたが、権利管理サーバ101bで管理している利用条件ID(利用条件管理テーブル500の利用条件ID502)を設定するようにしても良い。この場合、権利管理サーバ101bは、LT700を発行する際、LT700に利用条件ID502を追加する必要がある。端末装置102は、LT700に設定された利用条件ID502を用いて、UL1700に利用条件ID502を設定することができる。

#### 【0301】

また、本発明における実施の形態では、端末装置102が利用実績収集サーバ101eにUL1700を送信する際、PKIを用いたSACを用いる場合、および、相互認証を用いない、利用実績収集サーバ101eおよび端末装置102

間のセキュアな通信路を用いる場合の例を示したが、UL1700をコンテンツ鍵で暗号化して送信するようにしても良い。

#### 【0302】

また、本発明における実施の形態では、利用実績をUL1700に設定して、端末装置102から配信センター101に送信するようにしたが、これに限られるものではなく、端末装置102から配信センター101へのLT700の返却タイミングと連動させて、LT700を用いることによって、端末装置102から配信センター101に利用実績を送信するようにしても良い。

#### 【0303】

また、本発明における実施の形態では、コンテンツの利用部分を特定可能な情報として時刻情報を用いたが、これに限られるものではなく、コンテンツの先頭からの相対位置の把握が可能な情報であれば、時刻情報以外の何らかの位置情報（先頭からのバイト数など）を用いることも当然可能である。さらに、位置情報以外にも、少なくともコンテンツ内でユニークな情報（PCR1125aやPTS1043aなど）を含むTSパケット1100全体や、PESパケット1000全体を、端末装置102から利用実績収集サーバ101eに利用実績として送信するようにしても良い。これによれば、コンテンツ配信サーバ101cの送出時の処理、端末装置102での利用実績記録処理の負荷が軽減できる。加えて、時刻情報を用いる場合であっても、コンテンツの利用開始と終了のタイミングに利用実績を記録する場合のみならず、コンテンツの利用開始と継続時間とからコンテンツの利用終了を算出する方法など、コンテンツのどの部分を利用したかが把握可能な方法であれば、その他の方法を用いても良い。

#### 【0304】

また、本発明における実施の形態では、端末装置102のコンテンツ復号手段1521において利用実績を取得するか否かの判定を行ったが、コンテンツ利用手段1522において利用実績を取得するか否かの判定処理を行うようにしても良い。この場合、コンテンツ利用手段1522から第1の時刻情報記録手段1523に対して、利用実績として取得した第1の時刻情報が送信される。また、本発明における実施の形態2（図28）においても同様のことが言える。

**【0305】**

また、本発明における実施の形態では、権利管理サーバ101bが利用実績を収集する対象ユーザを動的に決定する場合の例を示したが、利用実績を収集する対象ユーザを予め決定しておくことにより、利用実績を収集する対象ユーザを静的に決定するようにしても良い。この場合、対象ユーザを記録したテーブルを、権利管理サーバ101b内のデータベース手段で保持しておけば良い。

**【0306】**

また、本発明における実施の形態では、配信センター101の構成について、複数のサーバ装置により実現される場合の例を示したが、これに限られるものではなく、例えば、複数の機能を1つのサーバ装置で実現するように構成しても良い。

**【0307】**

また、本発明における実施の形態では、端末装置102毎に利用実績を収集する場合の例を示したが、例えば、ホームネットワーク等の論理的または物理的なネットワーク内の、ホームサーバまたはチャネルサーバ単位で利用実績を収集するようにしても良い。

**【0308】**

さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、利用実績等を取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から取り込むようにすることもできる。

**【0309】****【発明の効果】**

本発明によれば、コンテンツにセキュアに設定された時刻情報を、端末装置で利用実績として記録し、この時刻情報を用いることにより、ユーザがコンテンツを利用したコンテンツ内の位置を特定するようにしているので、コンテンツプロバイダ、サービスプロバイダ等は、毎分視聴率、平均視聴率といった重要な情報をセキュアに得ることが可能となる。

**【0310】**

特に、MPEG-2 Systems など、コンテンツフォーマットに既存の時刻情報が存在し、運用等で当該時刻情報を柔軟に変更することが系統的に困難である場合においても、既存のシステムとの親和性が高いコンテンツ利用実績収集システムが構築できる。

#### 【0311】

さらに、早送り、巻戻しなどの特殊再生時には利用実績を取得しないようにすることにより、ユーザが実際にコンテンツを視聴した部分のみの利用実績が取得でき、より正確な視聴率調査が可能となる。

#### 【図面の簡単な説明】

##### 【図1】

本発明の実施の形態に係るコンテンツ利用実績収集システム1の全体の概略構成を示す図

##### 【図2】

本発明の実施の形態1に係る権利管理サーバ101bの構成を示す機能ブロック図

##### 【図3】

本発明の実施の形態1に係るユーザ情報DB201のテーブル構成を示す図

##### 【図4】

本発明の実施の形態1に係るコンテンツ鍵DB202のテーブル構成を示す図

##### 【図5】

本発明の実施の形態1に係る利用条件DB203のテーブル構成を示す図

##### 【図6】

本発明の実施の形態1に係る利用実績収集条件DB204のテーブル構成を示す図

##### 【図7】

本発明の実施の形態1に係るLT700の構成を示す図

##### 【図8】

本発明の実施の形態1に係る利用実績収集指示タグブロック704の構成を示す図

**【図 9】**

本発明の実施の形態 1 に係るコンテンツ配信サーバ 101c の構成を示す機能ブロック図

**【図 10】**

本発明の実施の形態 1 に係る PES パケット 1000 の概略構成を示す図

**【図 11】**

本発明の実施の形態 1 に係る TS パケット 1100 の概略構成を示す図

**【図 12】**

本発明の実施の形態 1 に係る利用実績収集サーバ 101e の構成を示す機能ブロック図

**【図 13】**

本発明の実施の形態 1 に係る第 1 の時刻情報と第 2 の時刻情報との関係を示す図

**【図 14】**

本発明の実施の形態 1 に係る利用実績 DB 1204 のテーブル構成を示す図

**【図 15】**

本発明の実施の形態 1 に係る端末装置 102 の構成を示す図

**【図 16】**

本発明の実施の形態 1 に係る ELI 1600 の構成を示す図

**【図 17】**

本発明の実施の形態 1 に係る UL 1700 の構成を示す図

**【図 18】**

本発明の実施の形態 1 に係る端末装置 102 における権利管理サーバ 101b からの LT 700 の取得処理を示すフローチャート

**【図 19】**

本発明の実施の形態 1 に係る権利管理サーバ 101b における LT 発行可否判定処理を示すフローチャート

**【図 20】**

本発明の実施の形態 1 に係る権利管理サーバ 101b における利用実績収集指

示生成処理を示すフローチャート

【図 2 1】

本発明の実施の形態 1 に係る端末装置 1 0 2 におけるコンテンツ利用処理および利用実績記録処理を示すフローチャート

【図 2 2】

本発明の実施の形態 1 に係る端末装置 1 0 2 におけるコンテンツ利用処理を示すフローチャート

【図 2 3】

本発明の実施の形態 1 に係る端末装置 1 0 2 における利用実績記録処理を示すフローチャート

【図 2 4】

本発明の実施の形態 1 に係るコンテンツ配信サーバ 1 0 1 c におけるコンテンツ送出処理を示すフローチャート

【図 2 5】

本発明の実施の形態 1 に係る端末装置 1 0 2 における利用実績収集サーバ 1 0 1 e に対する利用実績送信処理を示すフローチャート

【図 2 6】

本発明の実施の形態 2 に係るコンテンツ配信サーバ 1 0 1 c の構成を示す機能ブロック図

【図 2 7】

本発明の実施の形態 2 に係る利用実績収集サーバ 1 0 1 e の構成を示す機能ブロック図

【図 2 8】

本発明の実施の形態 2 に係る端末装置 1 0 2 の構成を示す図

【図 2 9】

本発明の実施の形態 2 に係る端末装置 1 0 2 におけるコンテンツ利用処理を示すフローチャート

【図 3 0】

本発明の実施の形態 2 に係る端末装置 1 0 2 における利用実績記録処理を示す

## フローチャート

## 【図 31】

本発明の実施の形態 2 に係るコンテンツ配信サーバ 101c におけるコンテンツ送出処理を示すフローチャート

## 【符号の説明】

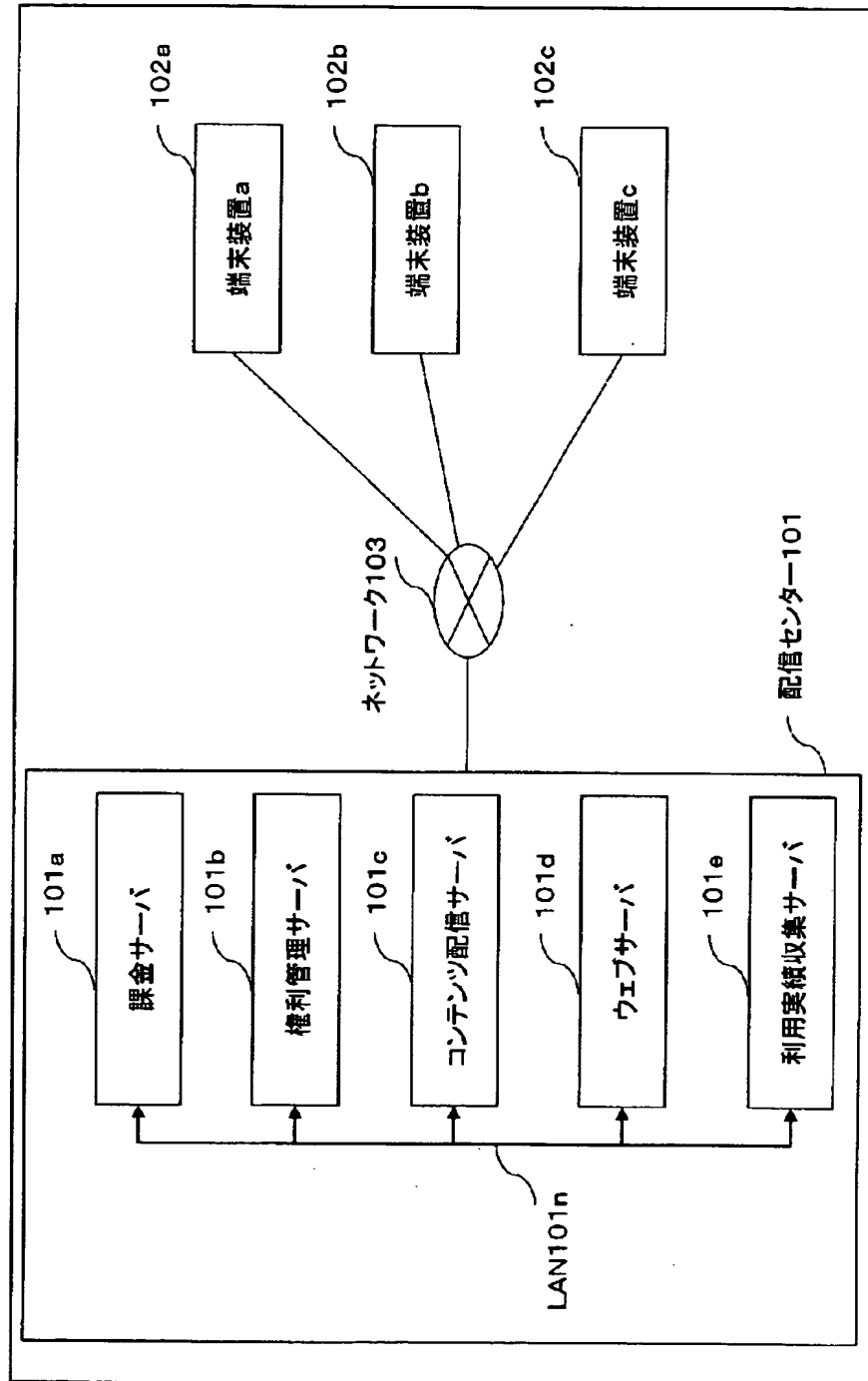
- 1、2 コンテンツ利用実績収集システム
- 101 配信センター
  - 101a 課金サーバ
  - 101b 権利管理サーバ
  - 101c コンテンツ配信サーバ
  - 101d ウェブサーバ
  - 101e 利用実績収集サーバ
  - 101n LAN
- 102 端末装置
- 103 ネットワーク
- 200 データベース部
  - 201 ユーザ情報DB
  - 202、911 コンテンツ鍵DB
  - 203 利用条件DB
  - 204 利用実績収集条件DB
- 210 ライセンス処理部
  - 211 利用実績収集指示手段
  - 212 ライセンス発行手段
  - 213 第1の送受信手段
- 901 コンテンツ取得要求受信手段
- 902 コンテンツ取得手段
- 903 コンテンツDB
- 904 コンテンツ多重化手段
- 905 コンテンツ暗号化手段

- 9 0 6 コンテンツ鍵供給手段
- 9 0 7 計時手段
- 9 0 8 第 1 の時刻情報付加手段
- 9 0 9 第 2 の時刻情報記録手段
- 9 1 0 コンテンツ送出手段
- 1 2 0 1 第 1 の時刻情報取得手段
- 1 2 0 2 第 2 の時刻情報取得手段
- 1 2 0 3、1 3 0 3、1 5 0 5 利用実績取得手段
- 1 2 0 4、1 3 0 4 利用実績 D B
- 1 5 0 0 権利管理部
- 1 5 0 1 第 2 の送受信手段
- 1 5 0 2 ライセンス取得手段
- 1 5 0 3 コンテンツ利用制御手段
- 1 5 0 4 セキュア D B
- 1 5 0 6 利用実績送信手段
- 1 5 2 0 コンテンツ利用部
- 1 5 2 1 コンテンツ復号手段
- 1 5 2 2 コンテンツ利用手段
- 1 5 2 3 第 1 の時刻情報記録手段
- 2 6 0 1 時刻情報付加手段
- 2 8 0 1 時刻情報算出手段

【書類名】

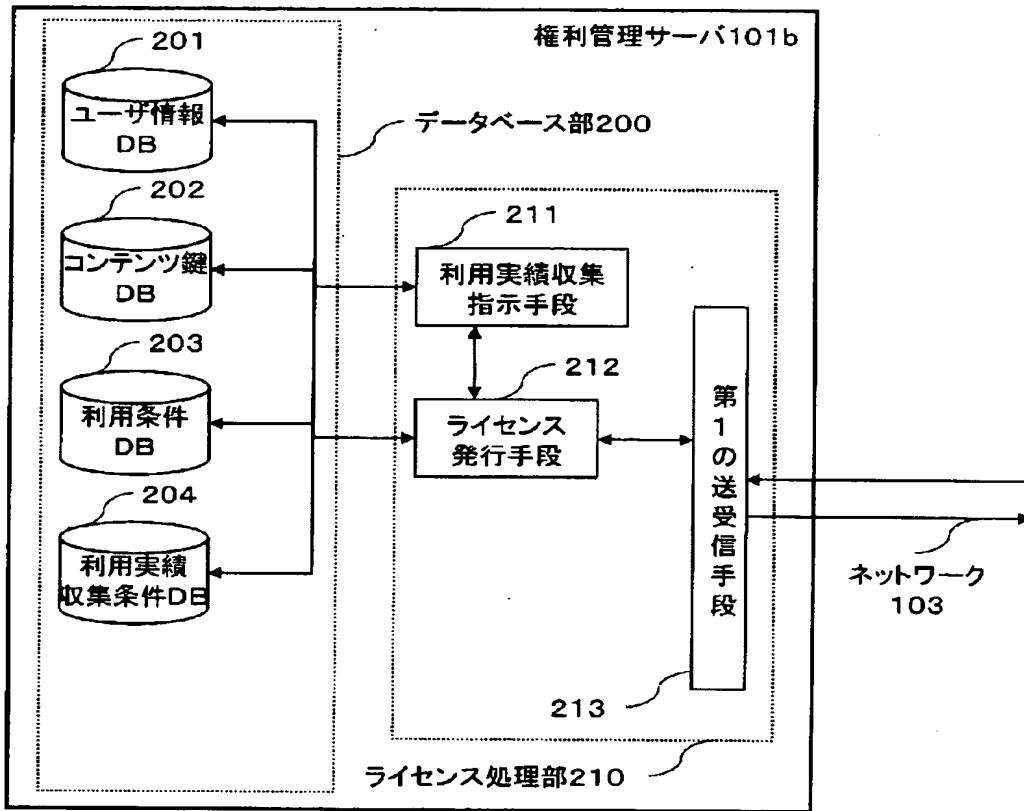
図面

【図 1】



コンテンツ利用実績収集システム1

【図 2】



【図 3】

ユーザID	端末ID	ユーザプロフィール	パフォーマンス
USER-ID-00001	TERMINAL-ID-00001	男性、31歳、...	実績収集OK
USER-ID-00002	TERMINAL-ID-12345 TERMINAL-ID-54321	女性、24歳、...	実績収集OK
USER-ID-00003	TERMINAL-ID-77777	女性、18歳、...	実績収集OK
USER-ID-00004	TERMINAL-ID-99999	男性、42歳、...	実績収集NG
...	...	...	...

ユーザ情報管理テーブル300

【図 4】

コンテンツID	コンテンツ鍵
CONTENT-ID-00001	0x1234567890abcdef
CONTENT-ID-00002	0x43195745a4098b4e
CONTENT-ID-00003	0x3970584ad3922247
CONTENT-ID-00004	0x2411197120121974
...	...

コンテンツ鍵管理テーブル400

【図 5】

501 ユーザID	502 利用条件ID	503 コンテンツID	504 有効期間	505 利用可能回数
USER-ID-00001	URUs-ID-00001	CONTENT-ID-00001	2002/12/31 ~ 2003/1/30	$\infty$
USER-ID-00002	URUs-ID-00002	CONTENT-ID-13452	2002/12/1 ~ 2002/12/31	5
USER-ID-00002	URUs-ID-10011	CONTENT-ID-99999	$\infty$	1
USER-ID-00003	URUs-ID-24024	CONTENT-ID-02804	2002/11/24 ~ 2002/12/20	$\infty$
...	...	...	...	...

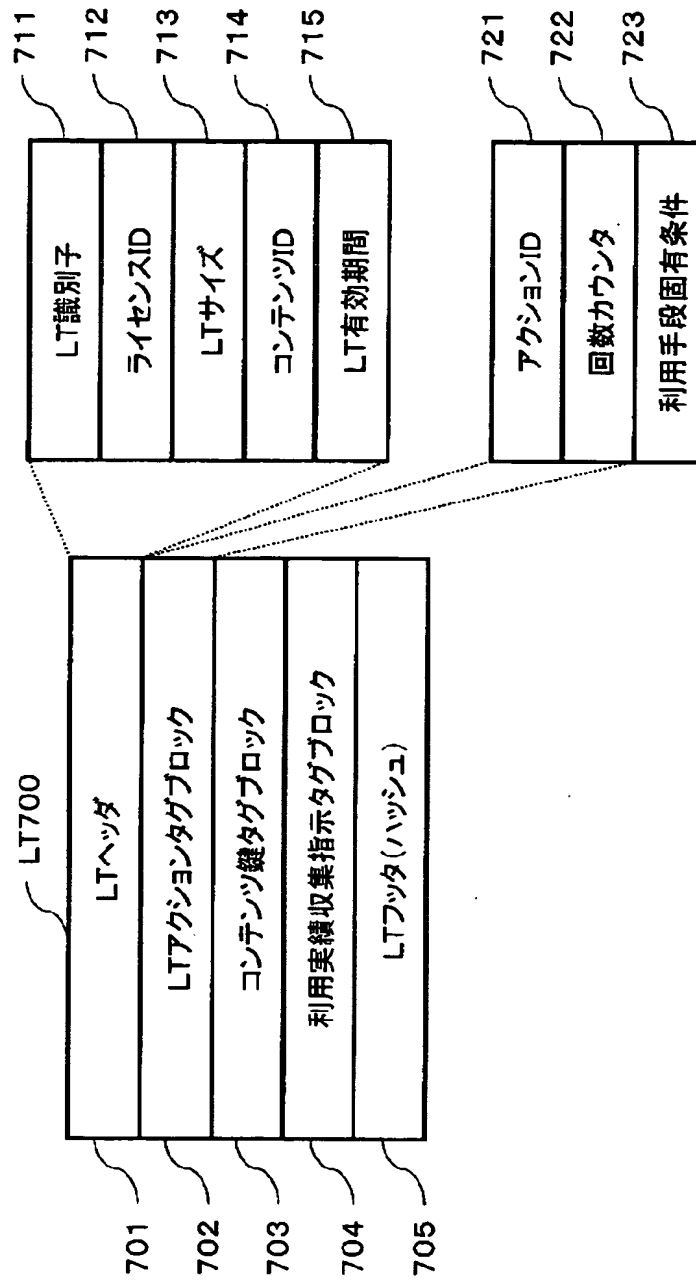
利用条件管理テーブル500

【図 6】

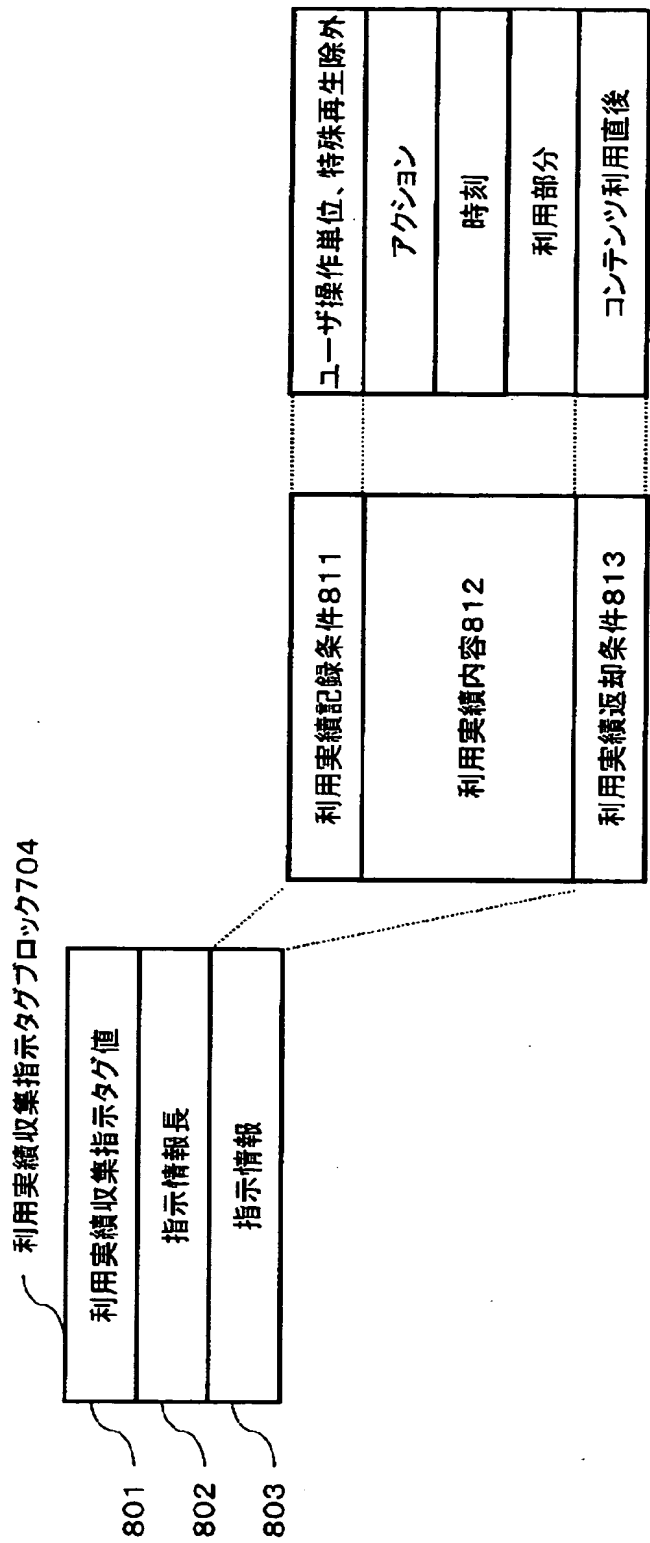
利用実績収集条件602					
601		603	604	605	606
コンテンツID	対象ユーザ決定条件	利用実績記録条件	利用実績内容	利用実績返却条件	
CONTENT-ID-00001	ランダム	コンテンツ単位	アクション、時刻	毎日5:00	
CONTENT-ID-00002	全ユーザ	ユーザ操作単位、 特殊再生あり	利用部分	ユーザ操作ごと	
CONTENT-ID-00003	プライバシポリシー	ユーザ操作単位、 特殊再生除外	アクション、時刻、利用部分	コンテンツ利用直後	
CONTENT-ID-00004	UR10権利以上	コンテンツ単位	アクション、時刻	LT返却時	
...	...	...	...	...	...

利用実績収集条件管理テーブル600

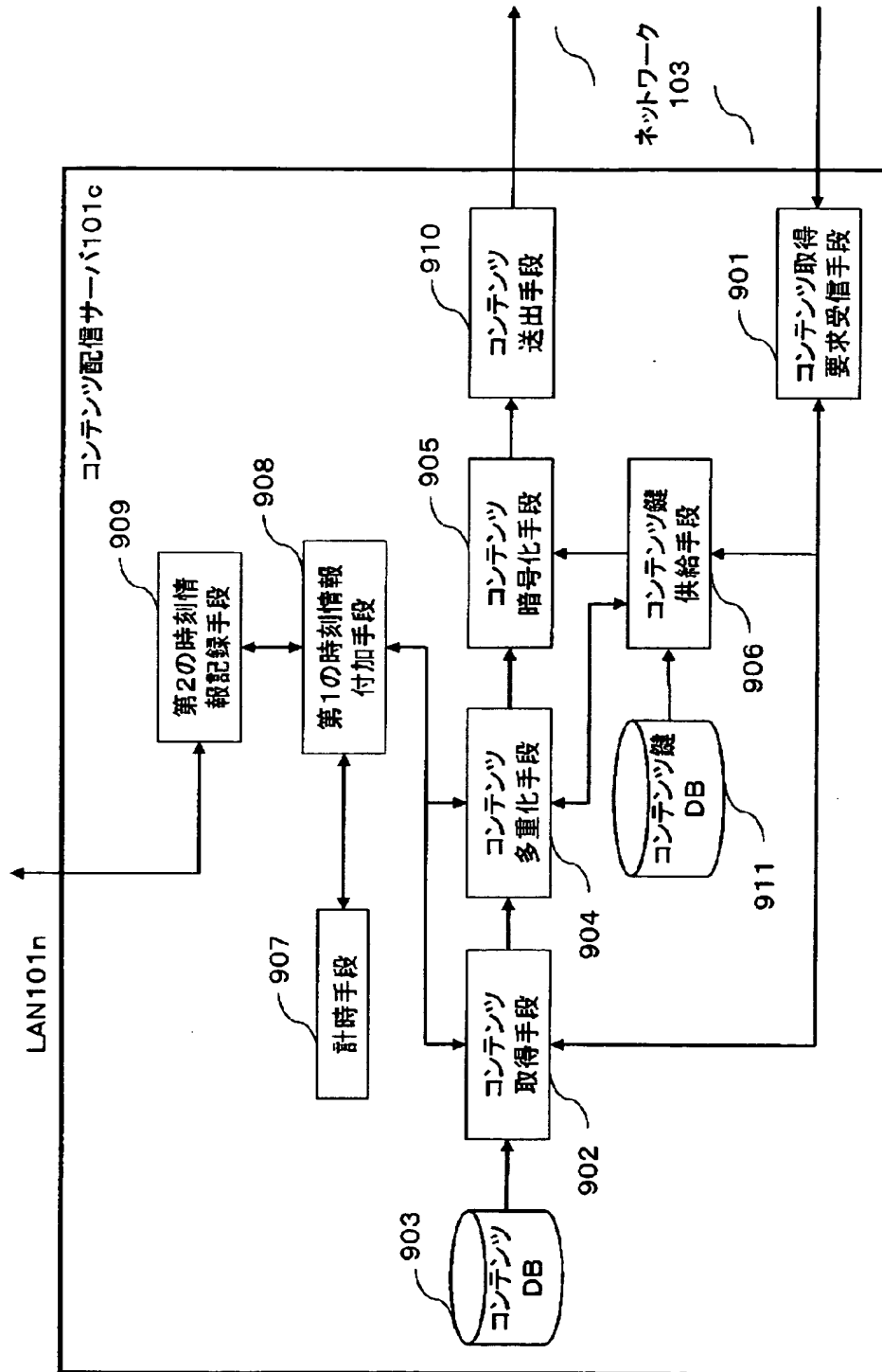
【図 7】



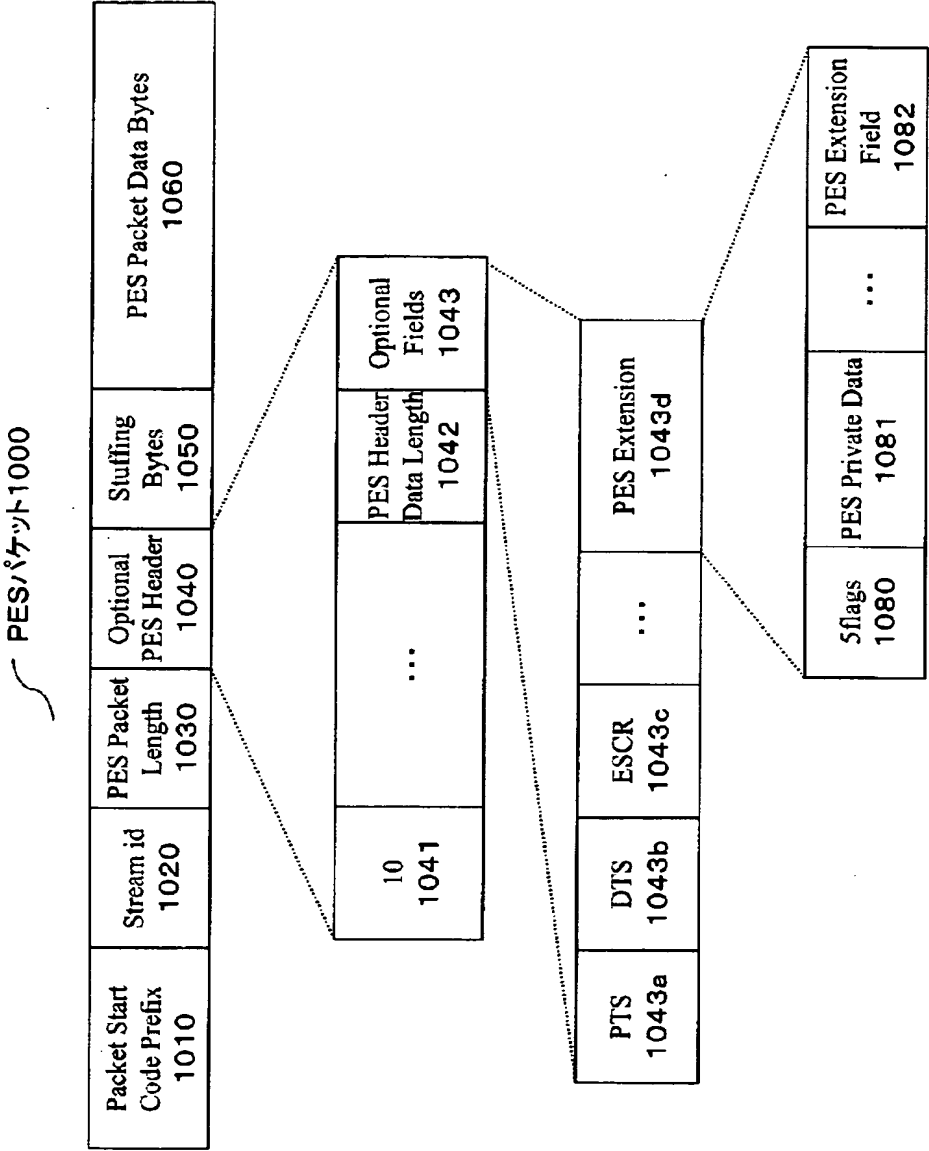
【図 8】



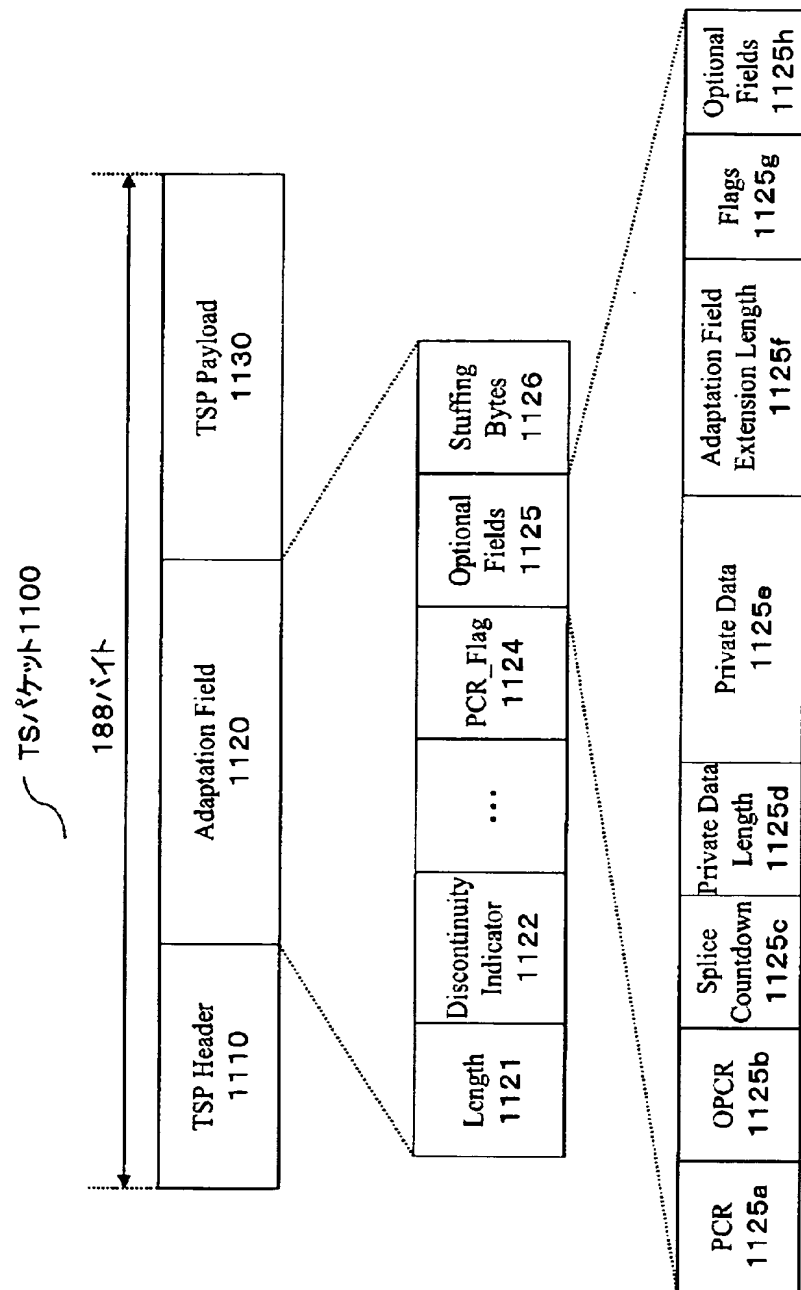
【図9】



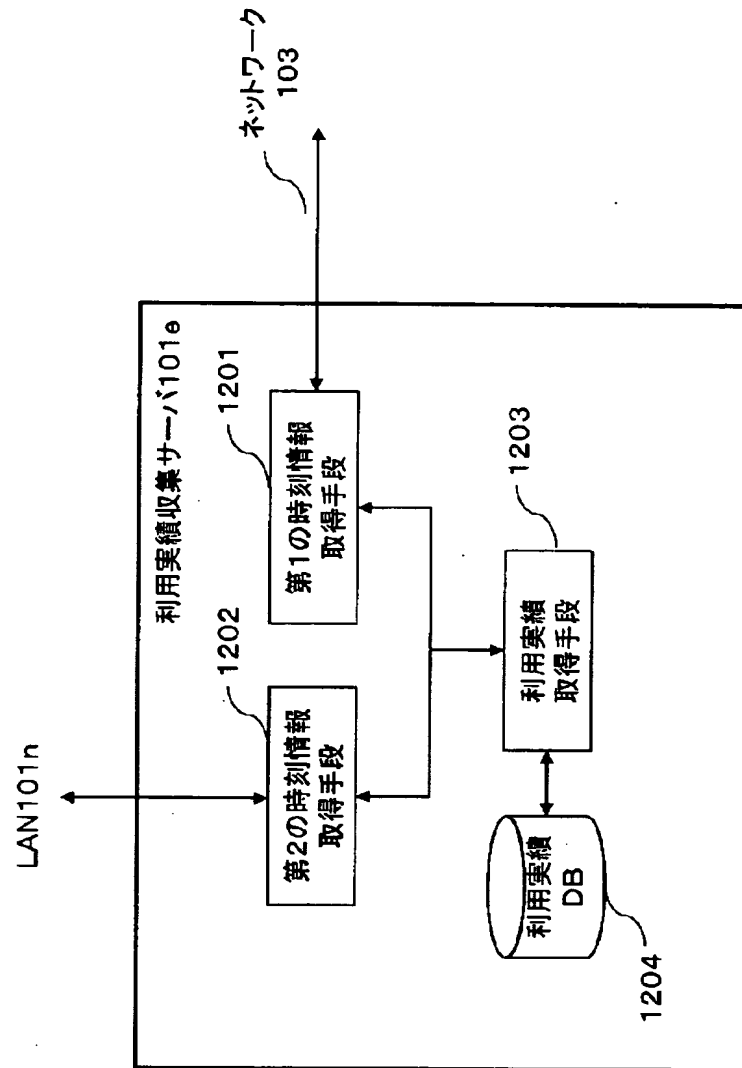
【図 10】



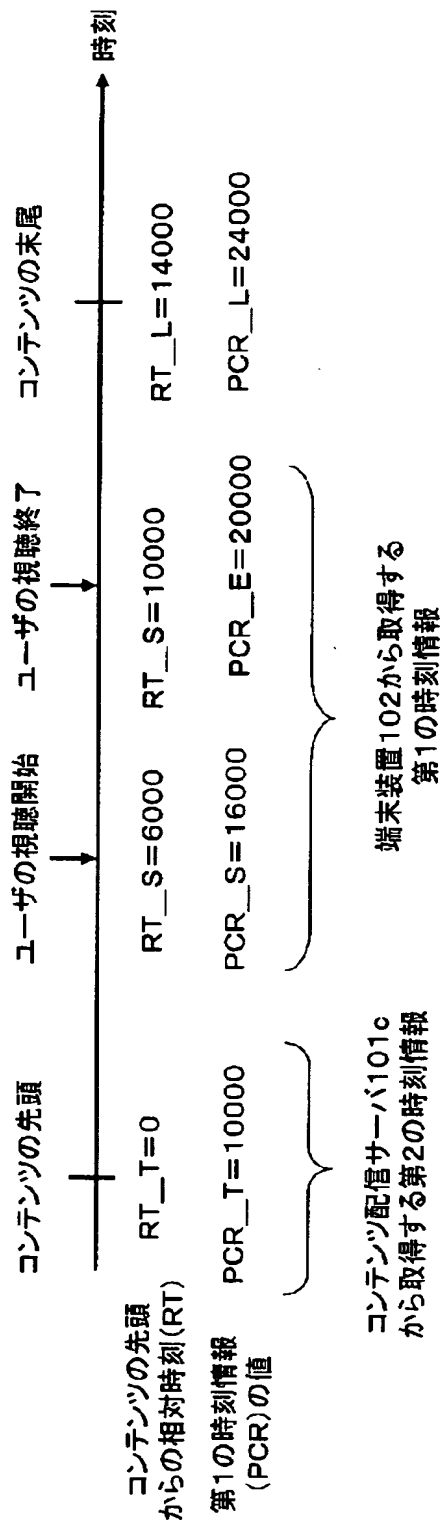
【図 11】



【図 12】



【図 13】



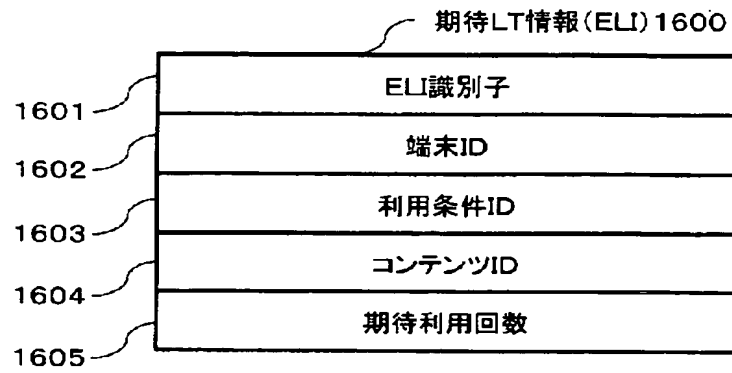
【図 14】

1401 ユーザID	1402 端末ID	1403 コンテンツID	1404 ライセンスID	1405 利用実績
USER-ID-00001	TERMINAL-ID-00001	CONTENT-ID-22222	LICENSE-ID-223606	Play::3970584, 3999999 Play::4010000, 4545454 ...
USER-ID-00002	TERMINAL-ID-11111	CONTENT-ID-33333	LICENSE-ID-898989	Play 2002/12/31 19:00:00 Play::1349309589, 1903434324 Fwd::1903434324, 4903438483 Rwd::4903438483, 4034356092 ...
...	...	...	...	...

利用実績管理テーブル1400



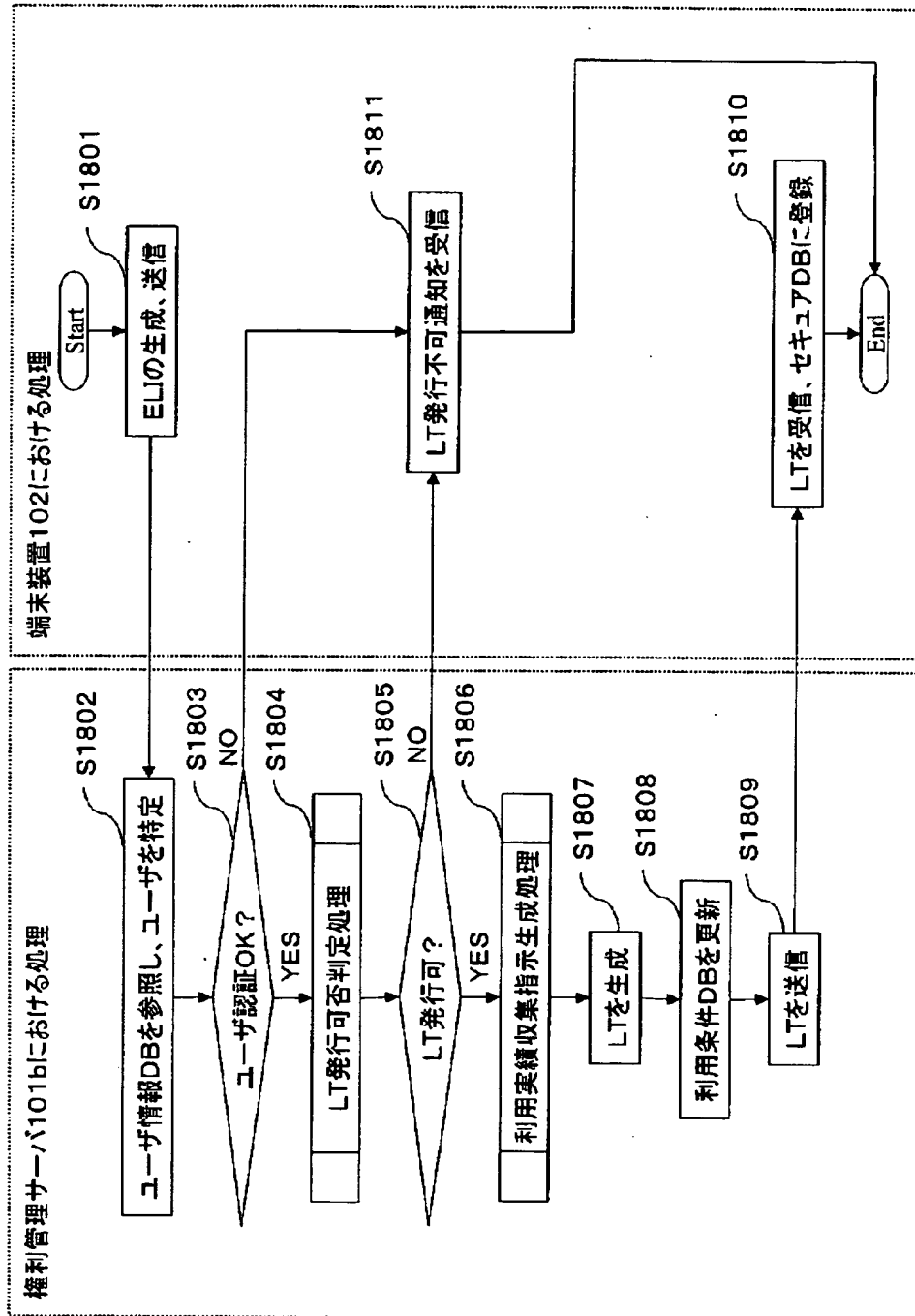
【図 16】



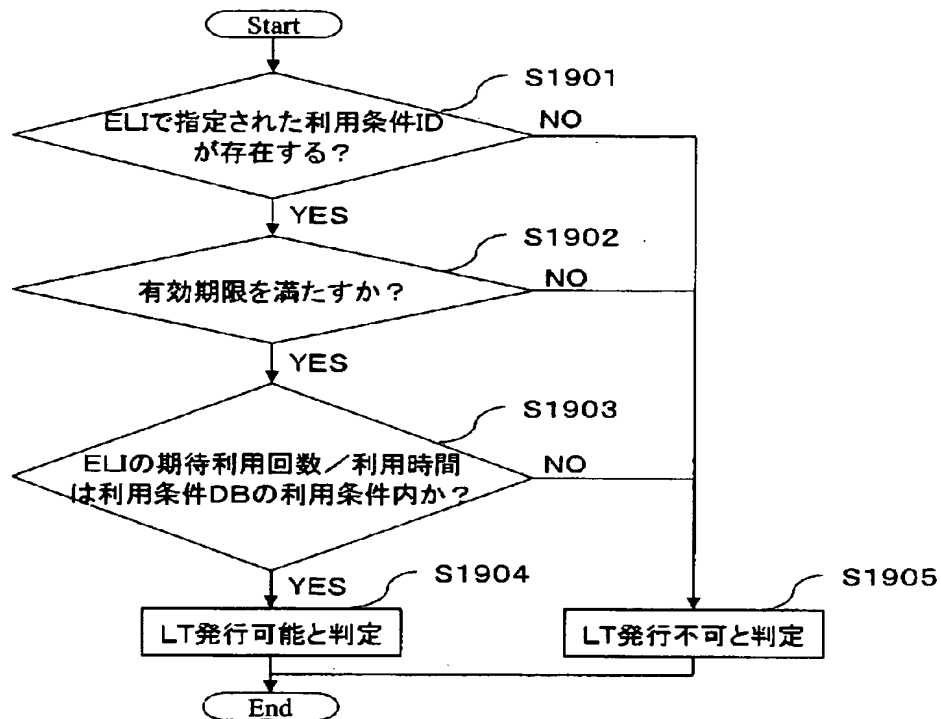
【図 17】

UL1700	UL識別子		BBDRM-UL
	ULサイズ		128
	ユーザID		USER-ID-00001
	端末ID		TERMINAL-ID-00001
	コンテンツID		CONTENT-ID-00001
	ライセンスID		LICENSE-ID-223606
	アクション種別		Play
	利用開始時刻		2003/1/1 10:00:00
	時刻情報個数		5
	時刻情報		
開始時刻情報1		13970584	
終了時刻情報1		13999999	
...		...	
開始時刻情報N		32141683	
終了時刻情報N		39705843970	

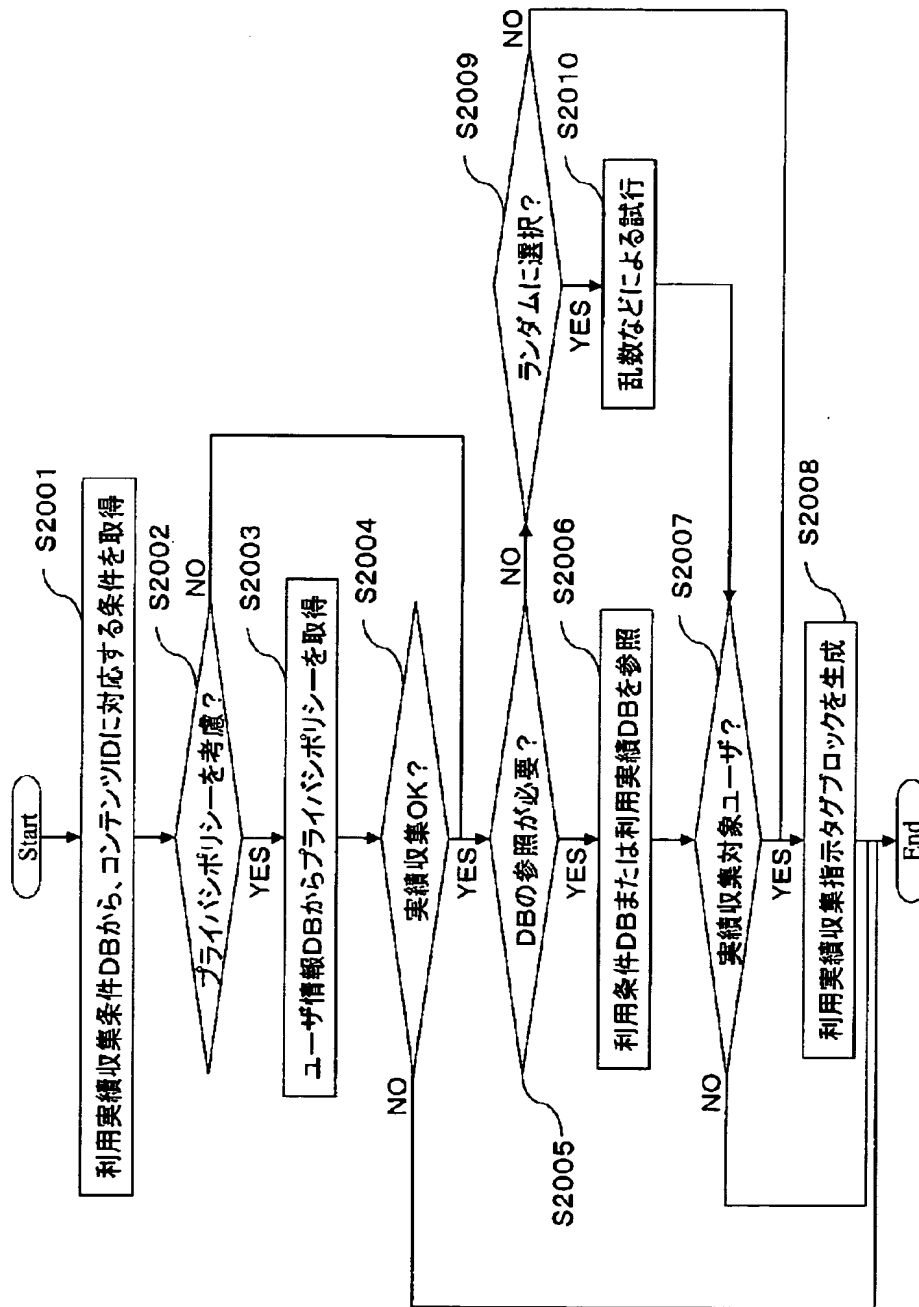
【図 18】



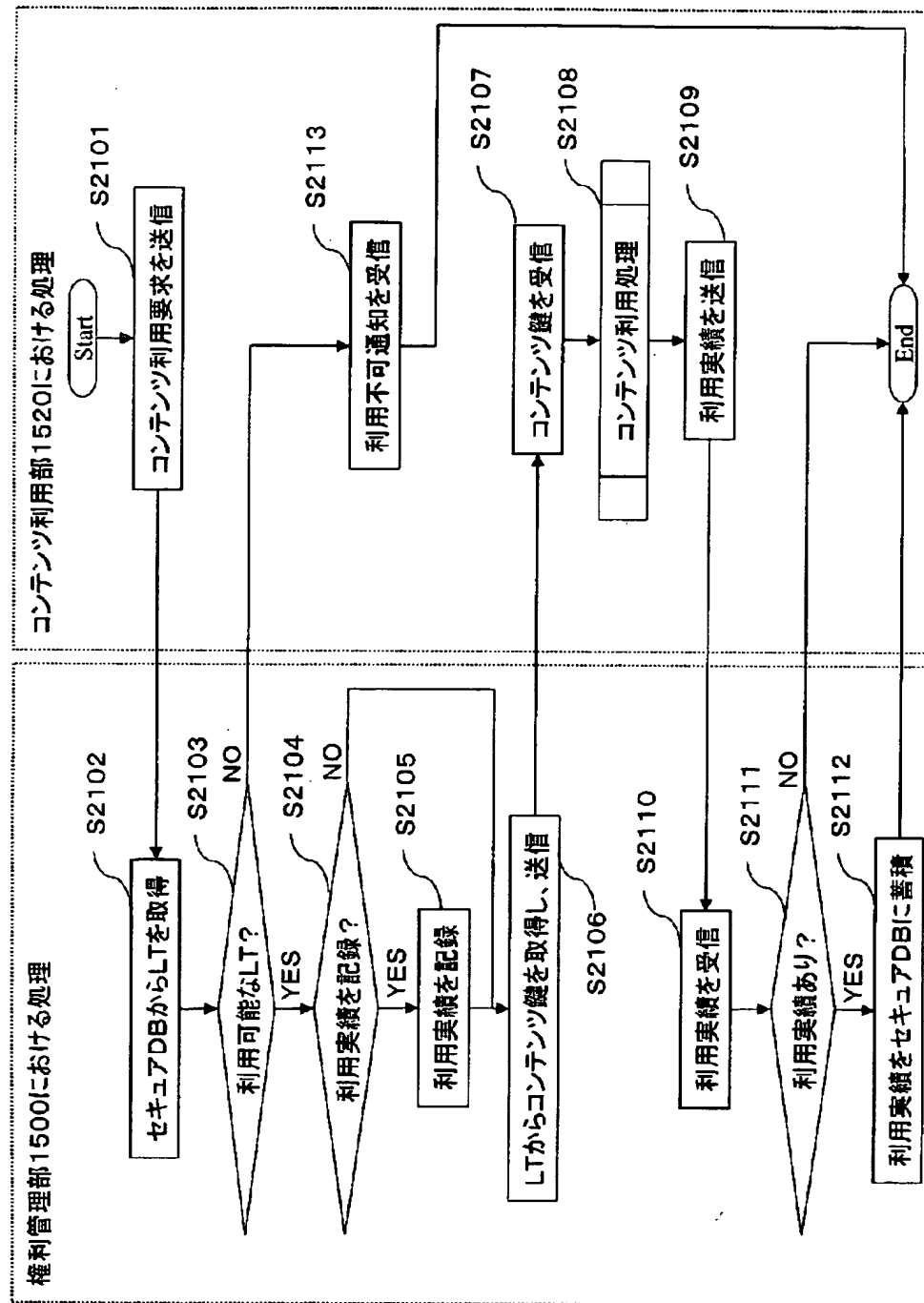
【図 19】



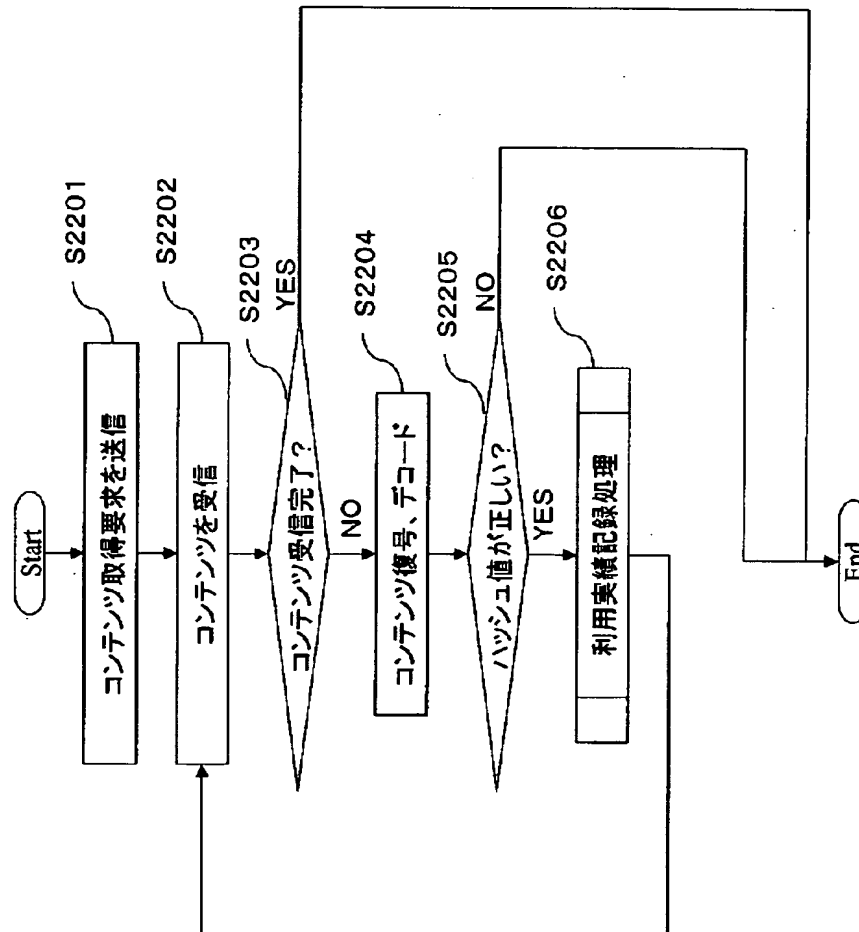
【図 20】



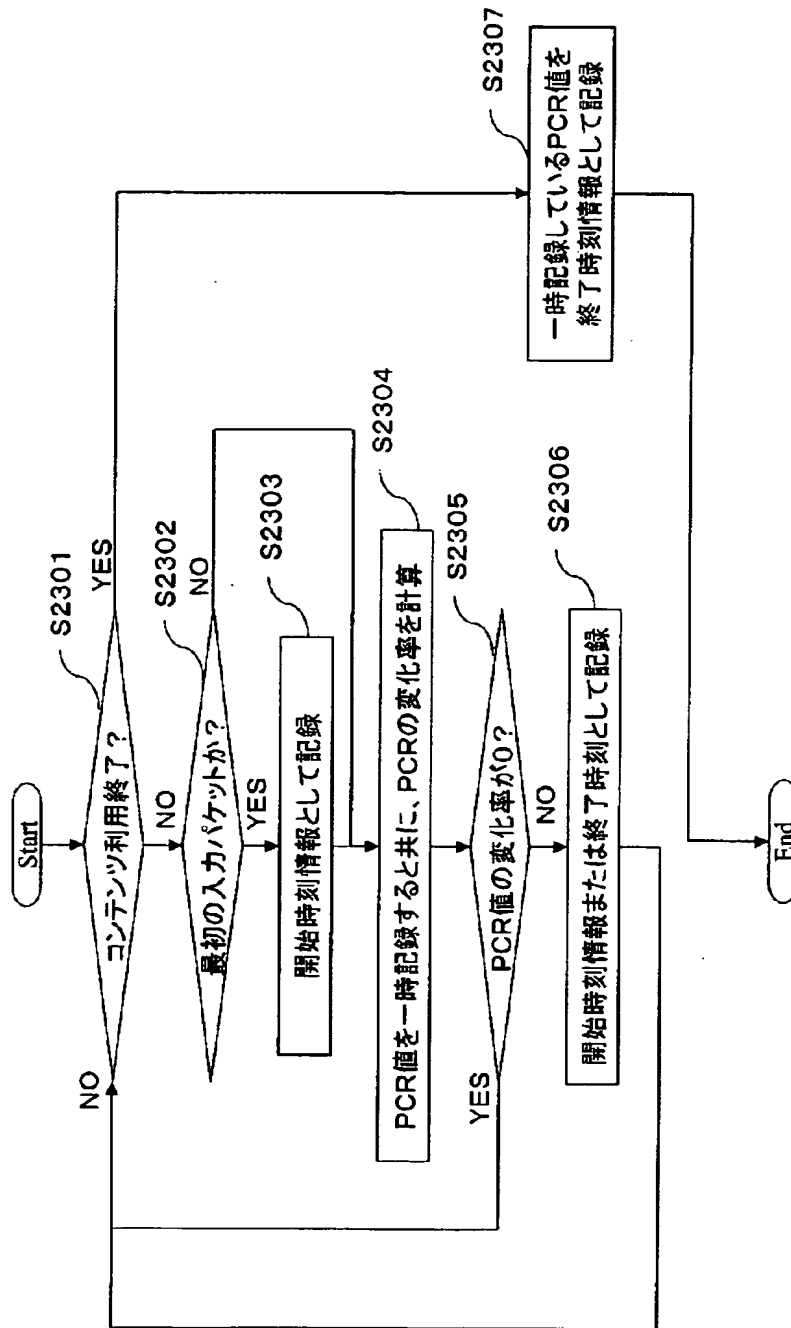
【図 21】



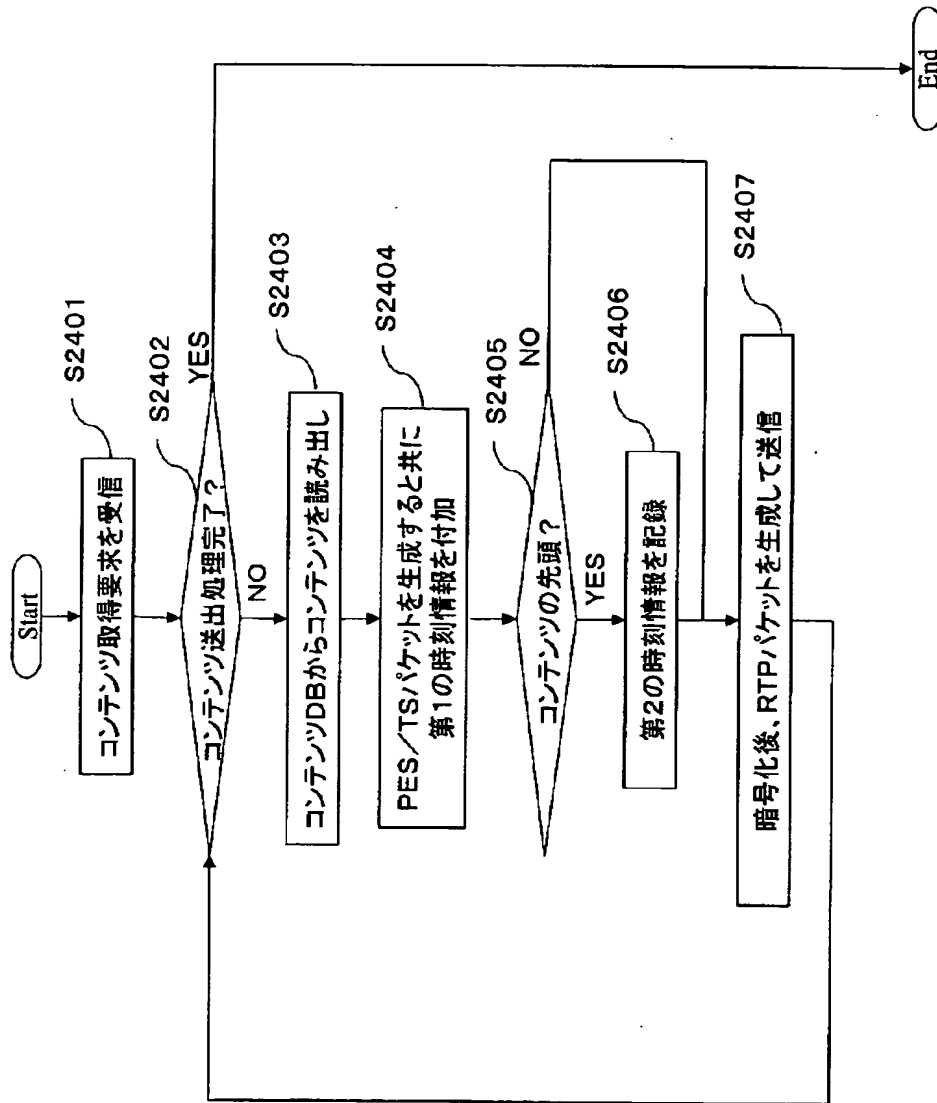
【図 22】



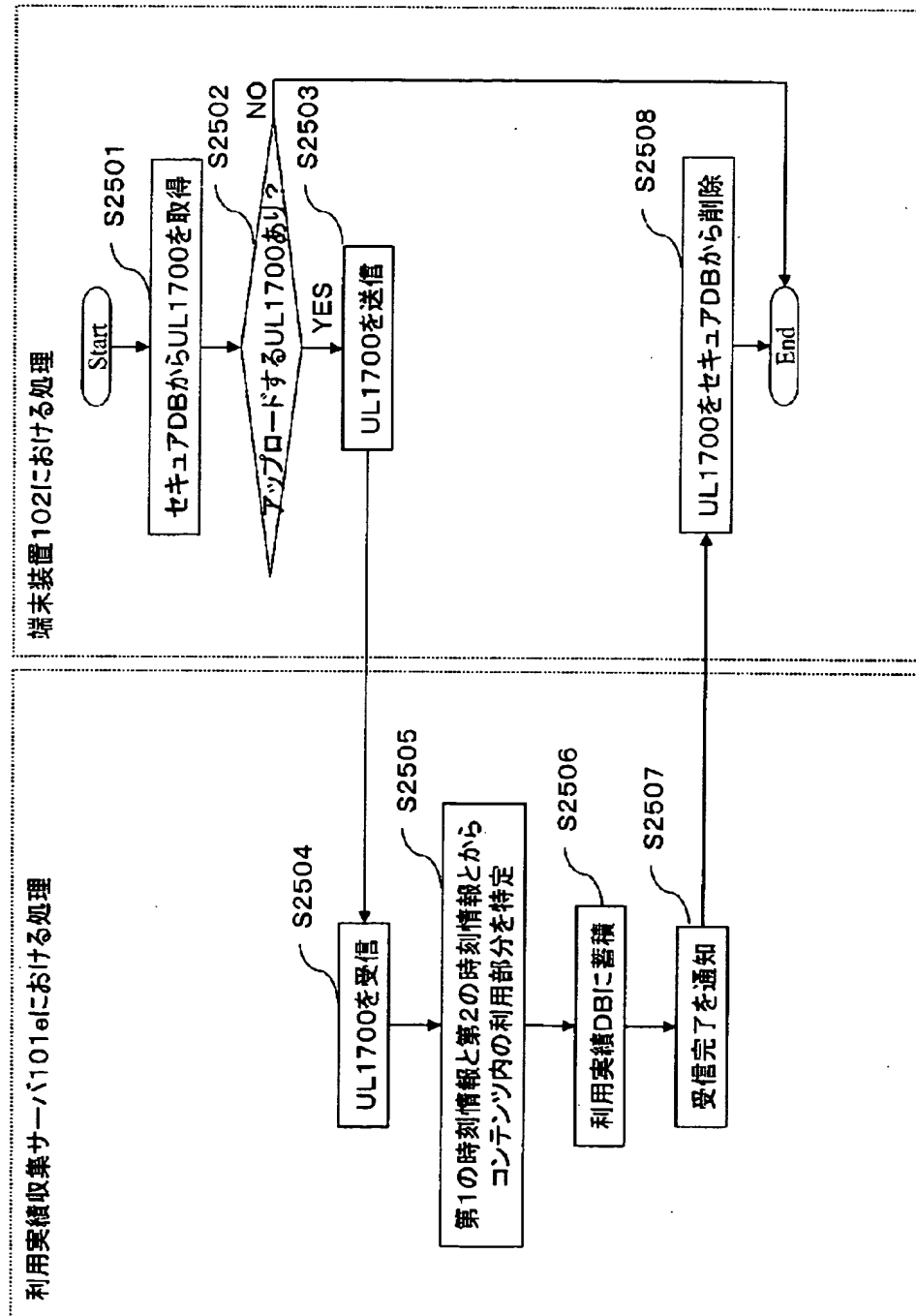
【図 23】



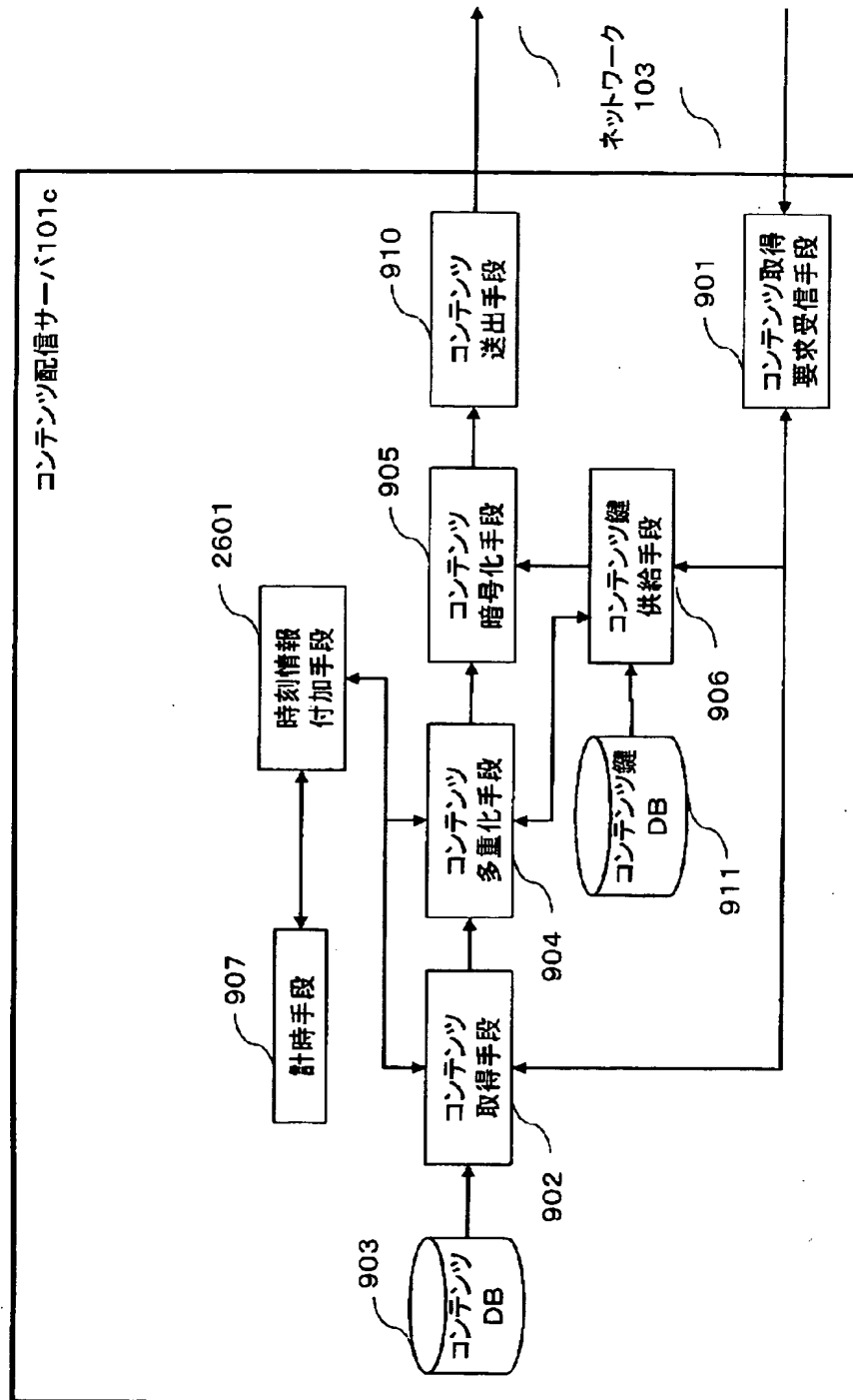
【図 24】



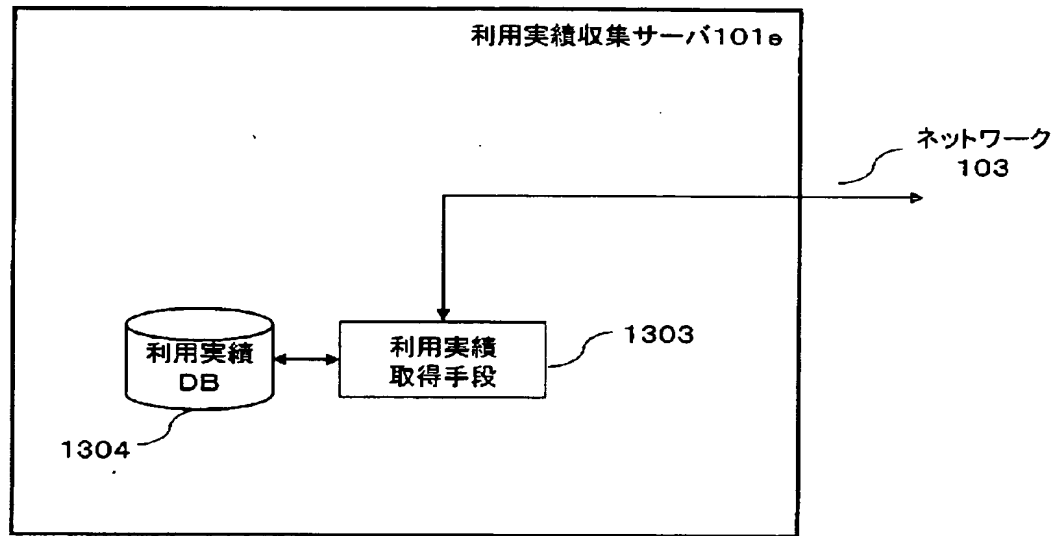
【図25】



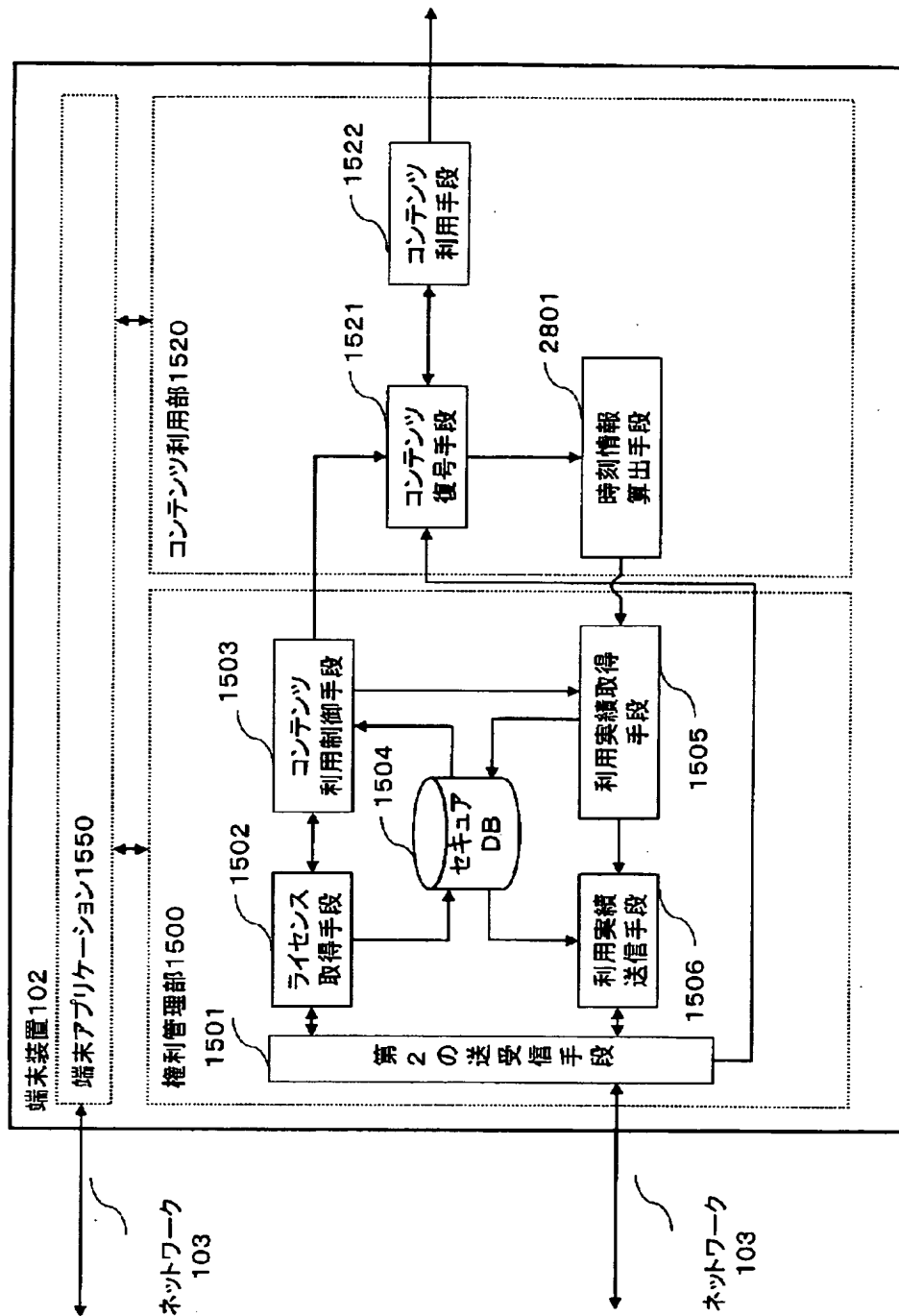
【図 26】



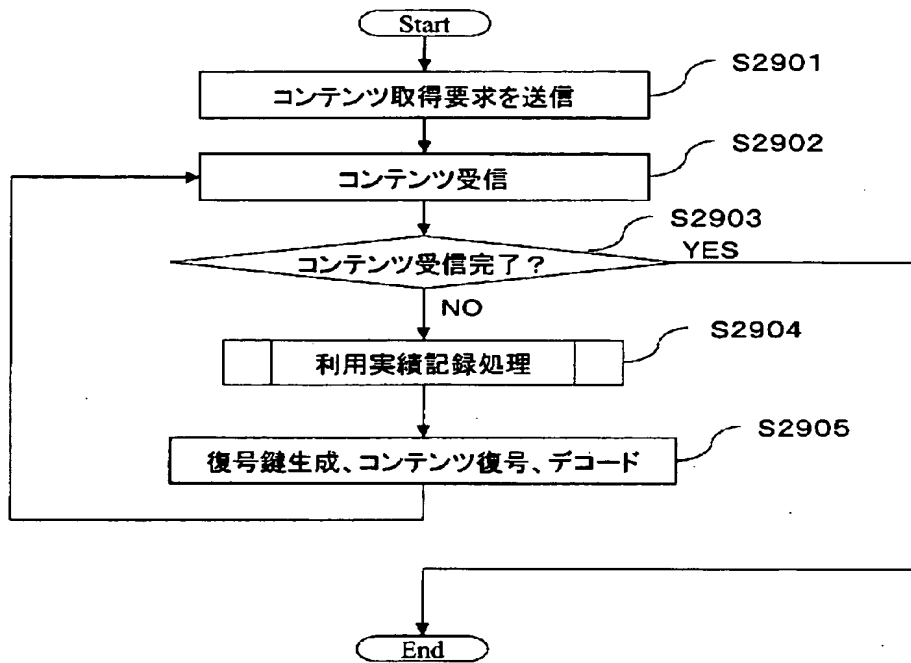
【図 27】



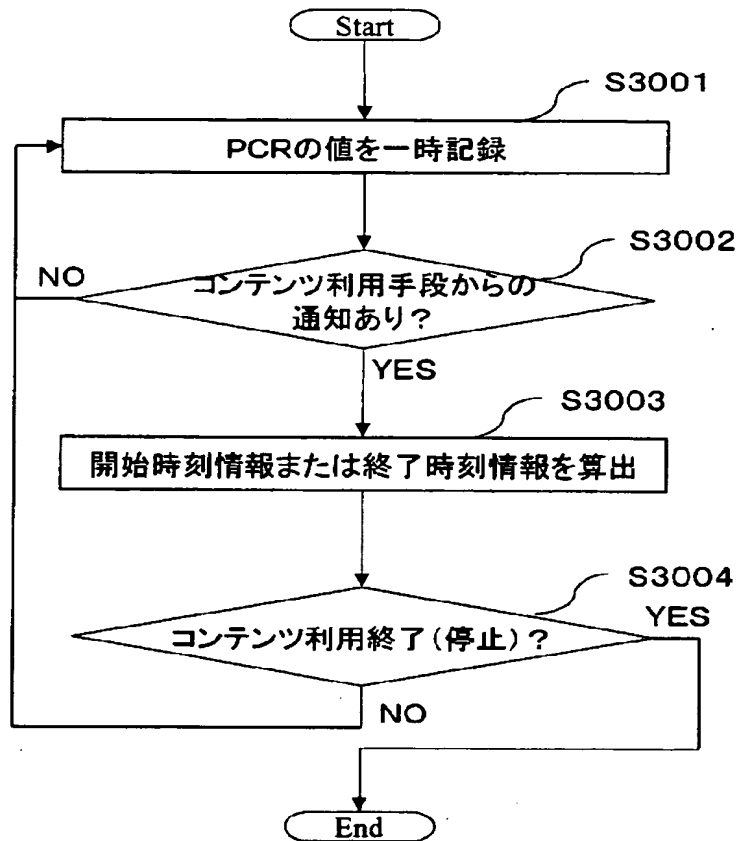
【図 28】



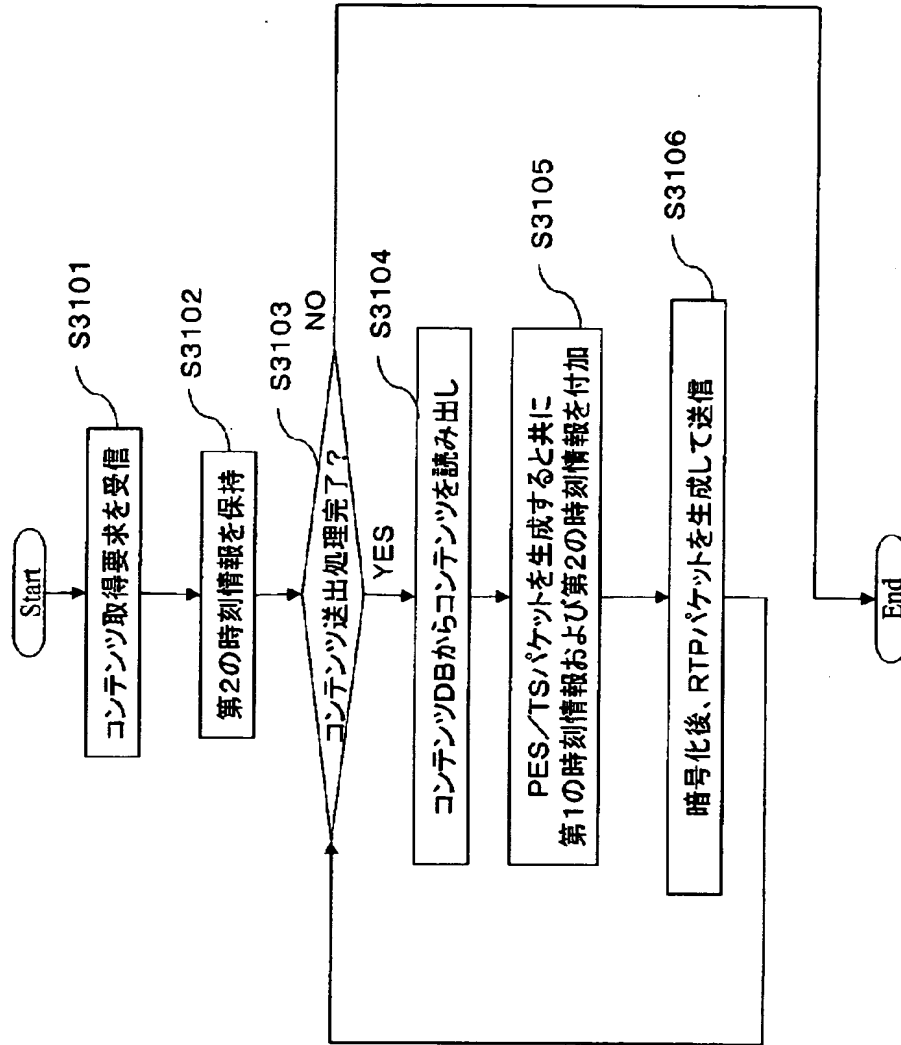
【図 29】



【図 30】



【図 31】



**【書類名】 要約書****【要約】**

**【課題】** ユーザによるコンテンツの利用部分を詳細かつセキュアに取得することにより、正確な視聴率調査が可能な利用実績収集システムを実現する。

**【解決手段】** コンテンツ配信サーバは、第1の時刻情報を生成する第1の時刻情報生成手段と、コンテンツの先頭での第1の時刻情報を第2の時刻情報として記録する第2の時刻情報記録手段とを備え、端末装置は、コンテンツに付加された第1の時刻情報を記録する第1の時刻情報記録手段と、第1の時刻情報を利用実績収集サーバに送信する利用実績送信手段とを備え、利用実績収集サーバは、端末装置から第1の時刻情報を取得する第1の時刻情報取得手段と、コンテンツ配信サーバから第2の時刻情報を取得する第2の時刻情報取得手段と、第1の時刻情報と第2の時刻情報とからコンテンツの利用部分を特定可能な時刻情報を算出する利用実績取得手段とを備える。

**【選択図】** 図1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 5 2 7 6 1
受付番号	5 0 3 0 0 3 3 0 7 4 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 3 月 3 日

< 認定情報・付加情報 >

【提出日】 平成 15 年 2 月 28 日

次頁無

特願 2003-052761

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社